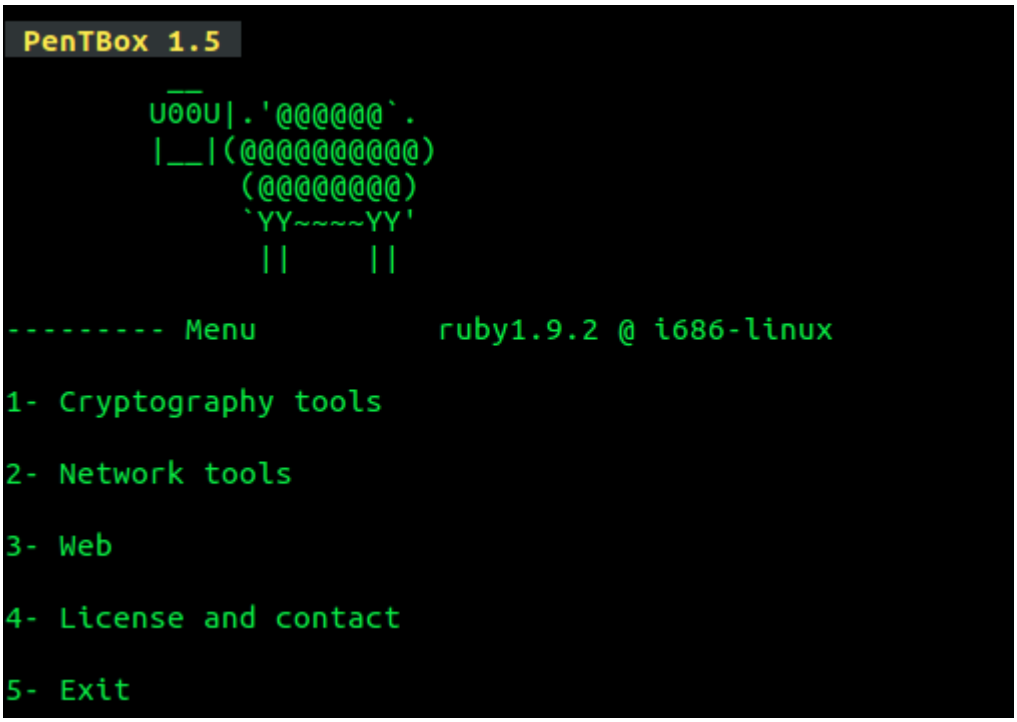
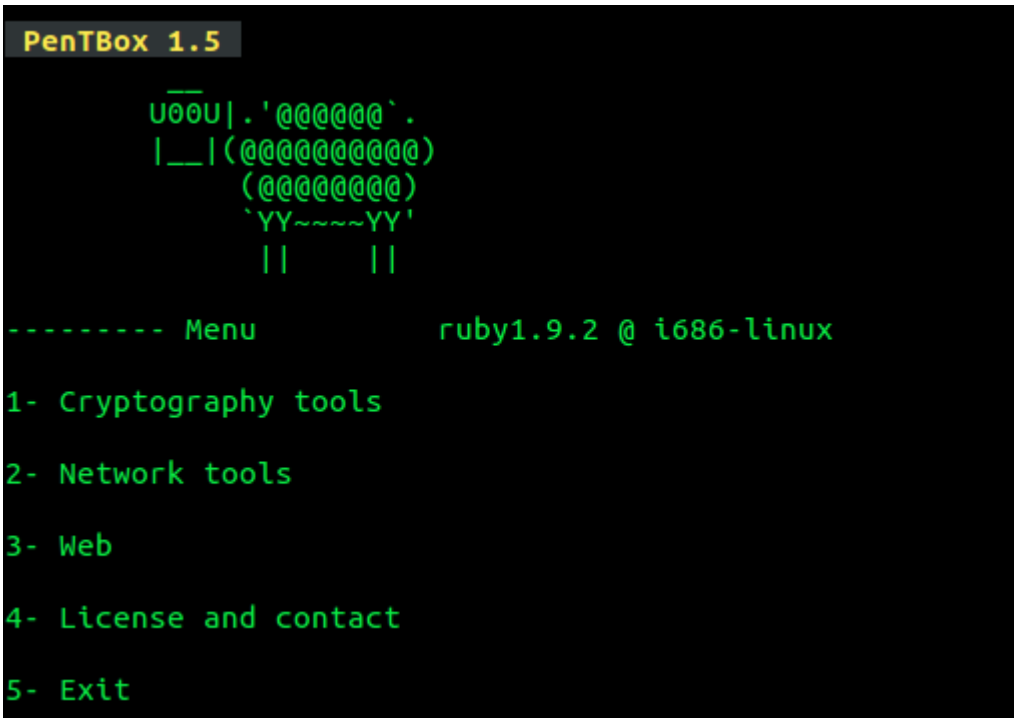
PenTBox

pentestlab.blog/category/tools/page/4

February 3, 2013



PenTBox is a security suite that can be used in penetration testing engagements to perform a variety of activities.Specifically these activities include from cracking hashes,DNS enumeration and stress testing to HTTP directory brute force.In this article we will see this tool in action and what kind of results we can have.



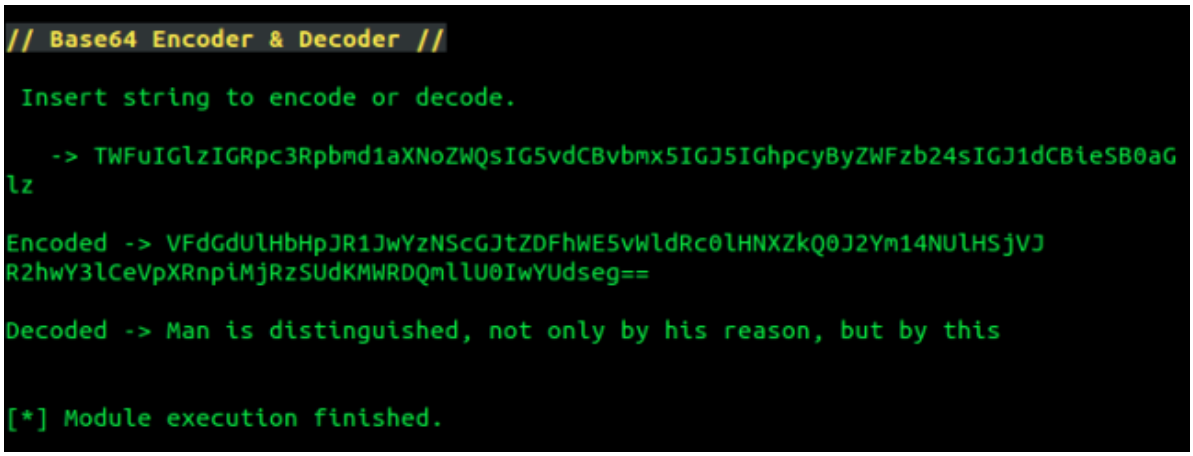
PenTbox – Menu

Cryptography Tools

PenTBox currently includes the following four cryptography tools:

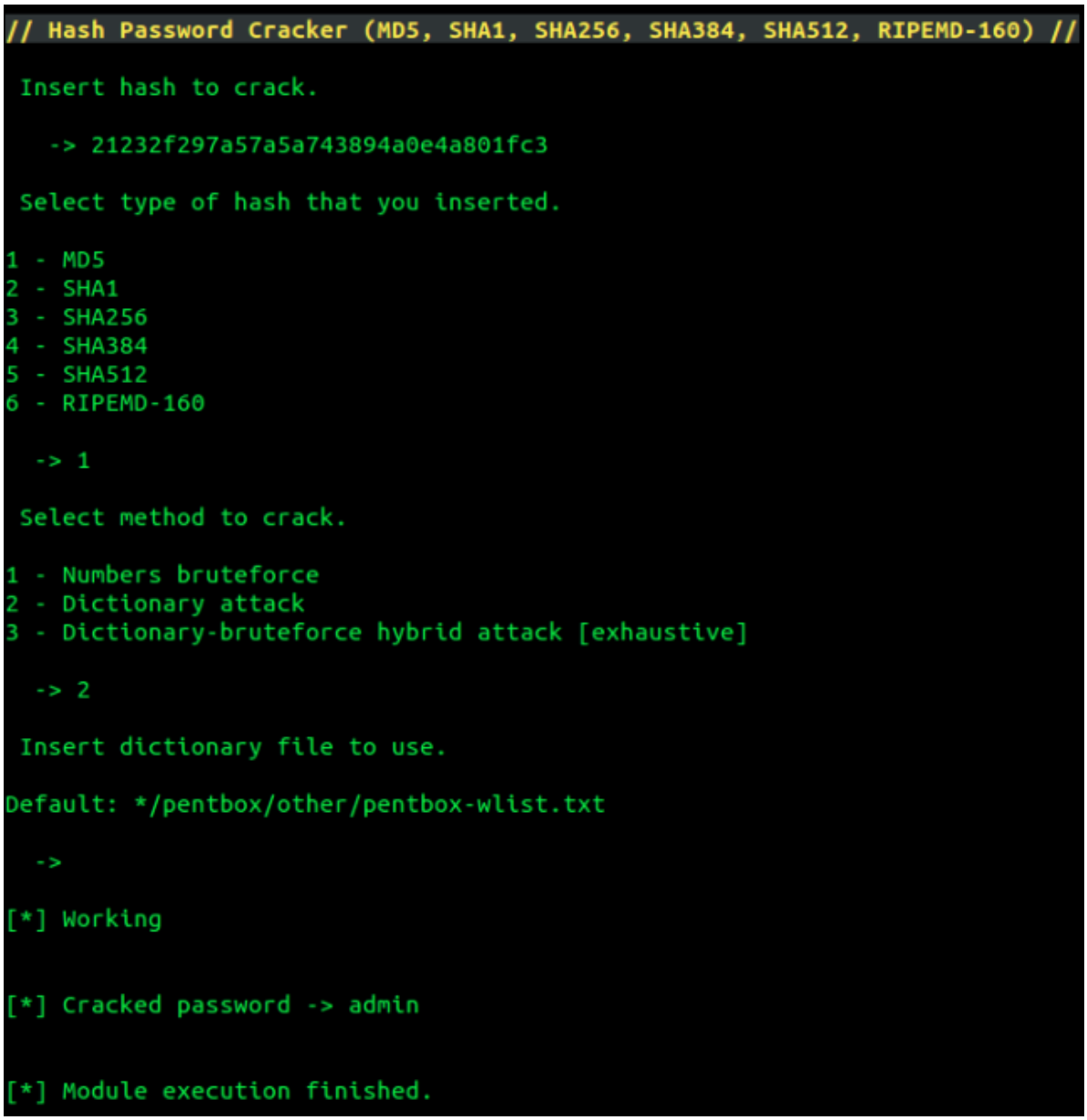
1. Base64 Encoder & Decoder
2. Multi-Digest
3. Hash Password Cracker
4. Secure Password Generator

Especially in web application penetration tests we often discover encoded Base64 strings.Such strings can contain important information that's why we need to have a decoder in our tool repository.Many tools now have integrated a Base64 Encoder-Decoder like Burp but PenTBox has also a Base64 decoder in his suite.



Base64 Encoder-Decoder

In case that we have obtain a password hash PenTBox provides a module that can crack different types of password hashes.The Hash Password Cracker can crack common password hashes very fast so it is a good practice to try it in any case.In the next image we can see that the Hash Password Cracker has managed to crack an MD5 hash.



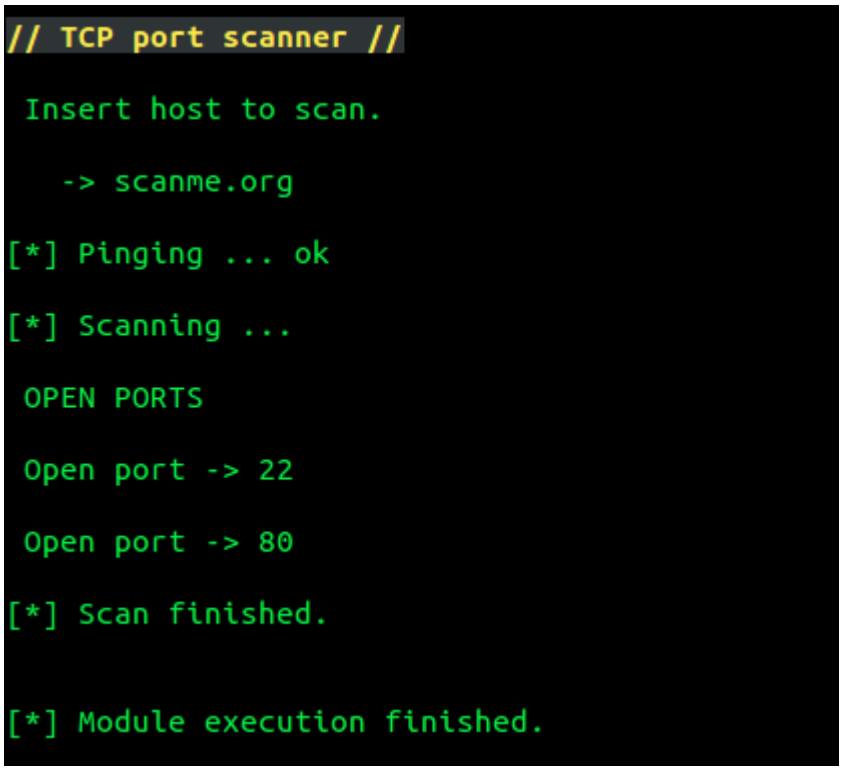
Hash Cracker Module – PenTBox

Network Tools

In this category there are tools for stress testing,fuzzing and information gathering.Specifically the tools that we can find here are the following:

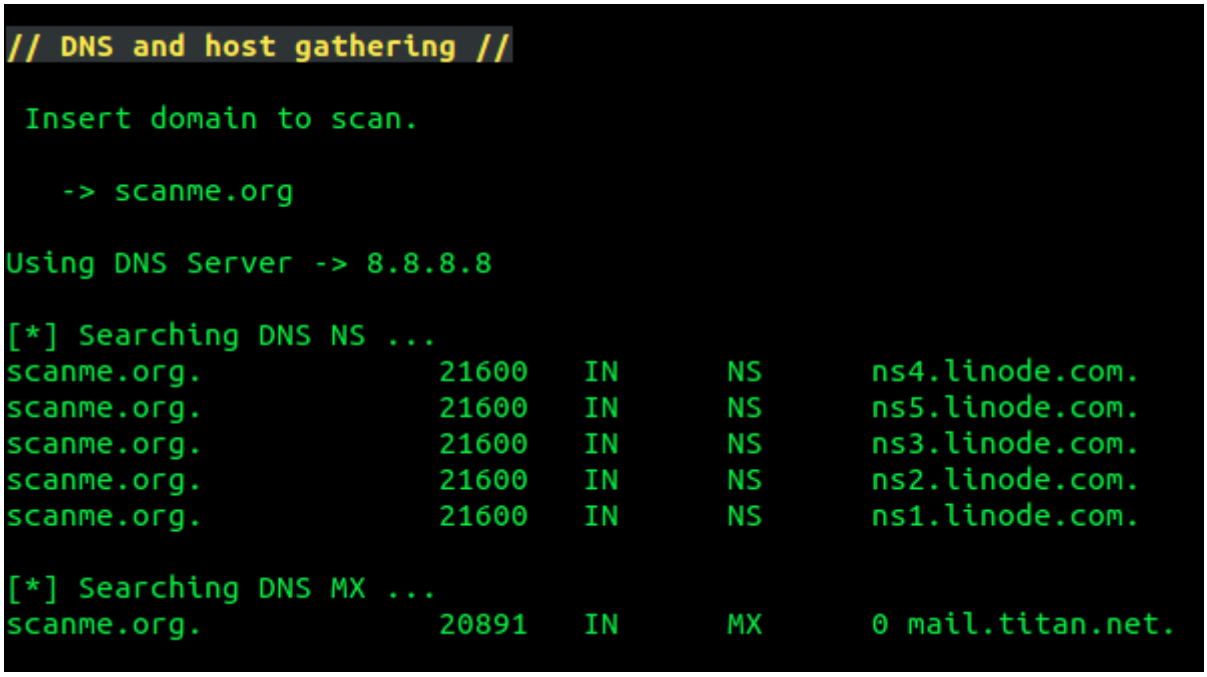
1. Net DoS Tester
2. TCP Port Scanner
3. Honeypot
4. Fuzzer
5. DNS and Host Gathering
6. MAC Address Geo-location

Even though that most penetration testers will use Nmap for their port scanning activities a simple TCP port scanner is available and through PenTBox.



PenTBox – TCP Port Scanner

Also a very fast module that can collect information about a specific host can be used for our information gathering activities.A sample of the output of this module can be seen in the next image:



DNS & Host Gathering – PenTBox

Web

PenTBox includes also and tools for web reconnaissance.Specifically it contains two tools for directory brute forcing and for discovering common files that exists in web servers.In the next image you can see the directory brute forcing tool in action.

```
// HTTP directory bruteforce //

 Insert url to bruteforce dirs.

 Example: http://example.com/
          http://example.com/dir1/dir2/

   -> http://scanme.org

 Use SSL? (y/N)

   -> N

 Determined values:
         Url: http://scanme.org/
         Host: scanme.org
         Port: 80
         SSL: false
         Path: /

[*] Bruteforcing dirs ...
    http://scanme.org// found - Response 200
    http://scanme.org//index found - Response 200
```

Directory Brute Force – PenTBox

Video:

Watch Video At: https://youtu.be/Gb7bwmnCuUQ

Conclusion

PenTBox is a framework that has written in ruby and offers some good tools that a penetration tester can use in an engagement.Of course there are better and more complex tools that can perform these activities but PenTBox offers the flexibility that contains many tools and it is very easy to use.For that reason this suite recommended for penetration testers with less experience.