Information gathering is generally a first step of ethical hacking/penetration testing, you need to get the maximum information about the victim because information is a key of success. As discussed before about information gathering in detail with different tools and technique like maltego and for DNS information gathering we have discussed DNSmap.

Information is weapon so in this article i will explain you how to get a information from DNS.

For this purpose i will use DNSenum, it is available on backtrack5 if you are using some other distribution and version than you can install it because it need only a perl, this may be a active perl or strawberry perl, you can run dnsenum on windows too. You can get the following information by using DNSenum.

- Host address
- Name server
- MX record
- Sub domains
- Whois performance
- Reverse lookup for netblocks
- Use google to do the job done

DNSenum is a very important tool to perform a quick enumeration step on penetration testing.

**Download**

**Ultimate Hacking**
Get hands on Ultimate Hacking at an information security course
info@edicinstitute.com

**Tutorial**

For this tutorial i am using backtrack, you can use some other distribution if you are using backtrack 5 than you can get DNSenum by click on Applications-->Backtrack-->Information gathering-->Network analysis-->DNS analysis-->DNSenum

By looking the options you can realize that the script has no many options and choices to use. It is very difficult to explain all options but i will try my best to explain most important options. Well the simple scan can start by just typing,
For a powerful scan use,

```
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl --enum google.com
```

For more power scan with sub domains

```
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl --enum -f -r google.com
```

I hope you are enjoying by using DNSenum.

Scanning and Enumeration – Second Step Of Ethical Hacking

Note: If you want to learn more about Linux and Windows based Penetration testing, you might want to subscribe our RSS feed or become our Facebook fan! You will get all the latest updates at both the places.

Related post

**BackTrack**
- Fern wifi Cracker – A Wireless Penetration Testing Tool
- DarkMYSQL– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5 – Postgresql Solved

**Backtrack5**
- DarkMYSQL– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5 – Postgresql Solved
- Complemento Backtrack 5 Toolkit
Ethical Hacking

for this purpose you need to make some changes on the kernel side, basically backtrack is based...

How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking—Your Way To The World Of IT Security · 2 days ago

revisualize

Is there a way to rename the bootloader to not read "Ubuntu, with Linux 2.6.38" and have it...

How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking—Your Way To The World Of IT Security · 2 days ago

Powered by Disqus