HACKINGLOOPS
LEARN ETHICAL HACKING & PENETRATION TESTING

MENU ≡

DNSRECON Tool Tutorial Hackingloops | KYB Tutorial 4

Share this...

Welcome friends to KYB (Know your Backtrack) Tutorial 4, today i am going to teach you another interesting DNS Information gathering tool i.e. DNSRECON Tool. DNSRECON Tool like other DNS tools used to enumerate the standard records of a domain like A, NS, SOA, MX etc. So friends lets learn all about DNSRECON Tool on Backtrack 5.

Dnsrecon KYB Tutorial 4 : Information gathering tool on Backtrack Linux

Below is the list of things that we can do using DNSRECON Tool:

- Top level domain expansion (Zone Walking and Zone Transfer)
- Reverse Lookup against IP range

- Perform general DNS query for NS,SOA and MX records (Standard Record Enumeration)
- Cache snooping against Name Servers
- Google Scanning for Sub Domains and Host

We can access **DNSRECON TOOL** over Backtrack by navigating below path:

> *Backtrack -> Information Gathering -> Network Analysis -> DNS Analysis -> dnsrecon*

Lets learn each of above things in detail and how to use DNSRECON tool to achieve the same:

1. Top level domain Expansion:

First of all we all should understand what are top level domains. A top-level domain (TLD) is one of the domains at the highest level in the hierarchical Domain Name System of the Internet. For ex: In www.mywebsite.com , .com is a top level domain. Usually expansion occurs for those websites which uses country codes as their top level domains ex: .in, .uk, .au etc. As the name suggests Top level domain Expansion means to expand your domain from one region to other which is also known as **Zone Transfer** and in case zones are not correctly configured we can extract almost all internal records of a domain which is also known as **Zone Walking**. So we can use DNS Recon for multiple purposes i.e. Zone Walking and Zone Transfer. Lets understand both of them in detail i.e. How we will use DNSRECON to exploit both of these features:

a. Zone Transfer : The security problem with DNS zone transfer is that it can be used to decipher the topology of a company’s network. Specifically when a user is trying to perform a zone transfer it sends a DNS query to list all DNS information like name servers,host names,MX and CNAME records, zone serial number, Time to

Live records etc. Due to the amount of information that can be obtained DNS zone transfer cannot be easily found in nowadays. However DNSRecon provides the ability to perform Zone Transfers and we can use following commands to perform Zone transfer:

> “ *./dnsrecon.py -d <mywebsite.com> -a*

or you can use below command :

> “ *./dnsrecon.py -d <mywebsite.com> -t axfr*

2. Reverse Lookup against IP range:

DNSRecon can perform a reverse lookup for PTR (Pointer) records against IPv4 and IPv6 address ranges.To run reverse lookup enumeration the command:

> “ *./dnsrecon.py -r <startIP>-<endIP>*

For Example :

```
./dnsrecon.py -r 192.168.5.100-192.168.5.200
```

Also reverse lookup can be performed against all ranges in SPF records with the command :

```
./dnsrecon.py -d <domain> -s
```

3. Domain Brute Force Enumeration:

For performing Domain Brute force technique, we have to give a name list and it will try to resolve the A,AAA and CNAME records against the domain by trying each entry one by one.
In order to perform domain brute force attack user needs to type below command:

```
./dnsrecon.py -d <domain> -D <namelist> -t brt
```

For example:

```
./dnsrecon.py -d hackingloops.com -D namelist.txt -t brt
```

4. Cache Snooping against name servers:

DNS cache snooping happens when the DNS server has a specific DNS record cached.This DNS record will often reveal plenty of information about the name servers and other DNS information.However DNS cache snooping does not happen quite often because servers normally do not cache DNS records.

The command that can be used to perform cache snooping is as follows:

> “ *./dnsrecon.py -t snoop -n server -D <dictionary file>*

For example :

> “ *./dnsrecon.py -t snoop -n <server IP address> -D dictionary.txt*

5. Standard Records Enumeration:

Standard Enumeration is generally used to gather information about NameServers,SOA and MX records. In order to perform standard enumeration you can use below command:

> “ *./dnsrecon.py -d <domain>*

For example:

> “ *./dnsrecon.py -d hackingloops.com*

There are lot of other options that DNSRECON tool provides. It is an extremely useful tool to gather plenty of information about DNS records.

Thats all for today. If you have any doubts feel free to ask. Don’t forget to join us at Facebook in order to recent updates.

Filed Under: Ethical Hacking, Hack Tools, Information Gathering, Open Source Penetration Testing Tools, Penetration Testing Tools
Tagged With: BEH, BEHC, Born Hackers Club, DNSRECON, DNSRECON Tool, DNSRECON tool tutorial, DNSRECON tutorial, Hacking Basics, Hacking School, Know Your Backtrack, KYB, Online Ethical Hacking Class, Website Hacking

‹ Previous Post

How to Share Remote Screens and Control PC Without Any Software in Windows

Next Post ›

Injection Attacks Tutorial – OWASP #1 Vulnerabilty – Part 1

Did you enjoy this post?

Would you like to join our Insider's List and be notified when we post something or get FREE exclusive content?

JOIN OUR INSIDER'S LIST

Leave a Reply

Comment

Name *

Email *

Website

POST COMMENT

Don't Know Where To

Get Started?

I'll show you exactly how to get started Pentesting!
Show Me How!

RECENT POSTS

- Top Application Security Certifications for Pros
- The Most In Demand Blockchain Security Certifications
- Flashlight – Network Information Gathering and Data Filtration Tool
- Why Threat Hunting Certifications Will Change Your Life
- Who wins? Hyper-V vs. VirtualBox

BECOME A MEMBER

JOIN US!
BECOME A MEMBER!
PENETRATION TESTING 101. YOUR BLUEPRINT AND STEP-BY-STEP GUIDE!

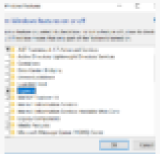
FEATURED POSTS

Top Application Security Certifications for Pros

The Most In Demand Blockchain Security Certifications

Flashlight – Network Information Gathering and Data Filtration Tool

Why Threat Hunting Certifications Will Change Your Life



Who wins? Hyper-V vs. VirtualBox

ETHICAL HACKING PRACTICE TESTS

Ethical Hacking Practice Test 7

CEH Certification Overview

Ethical Hacking Practice Test 6 – Footprinting Fundamentals Level1

CEH Practice Test 5 – Footprinting Fundamentals Level 0

CEH Practice Test 4 – Ethical Hacking Fundamentals Level 2

CONTACT US

PRIVACY POLICY

DISCLAIMER

500 Westover Dr #8208 Sanford NC 27330