How-to: DNS Enumeration

25-04-2010

Author: Mohd Izhar Ali
Email: johncrackernet@yahoo.com
Website: http://johncrackernet.blogspot.com

Table of Contents

1. Introduction

A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

The first step of penetration testing or more accurately called information security testing is information gathering. Information gathering is part of the preparatory pre-attack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of finding ways to intrude into that environment. Information gathering can reveal system vulnerabilities and identify the ease with which they can be exploited. This is the easiest way for attacker to gather information about computer systems and the companies they belong to. The purpose of this phase is to learn as much as you can about a system, its remote access capabilities, its ports and services, and any specific aspects of its security.

Using a combination of tools and techniques, attackers can take an unknown entity and reduce it to a specific range of domain names, network blocks, subnets, routers, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture. Although there are many types of information gathering techniques, they are primarily aimed at discovering information related to the following environments: Internet, intranet, remote access, and extranet.

2. DNS Enumeration

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems. There are a lot of tools that can be used to gain information for performing DNS enumeration. The examples of tool that can be used for DNS enumeration are NSlookup, DNSstuff, American Registry for Internet Numbers (ARIN), and Whois. To enumerate DNS, you must have understanding about DNS and how it works.

You must have knowledge about DNS records. The list of DNS record provides an overview of types of resource records (database records) stored in the zone files of the Domain Name System (DNS). The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses. In these domain servers, different record types are used for different purposes. The following list describes the common DNS record types and their use:

- *A (address)*—Maps a host name to an IP address
- *SOA (Start of Authority)*—Identifies the DNS server responsible for the domain information
- *CNAME (canonical name)*—Provides additional names or aliases for the address record
- *MX (mail exchange)*—Identifies the mail server for the domain
- *SRV (service)*—Identifies services such as directory services
- *PTR (pointer)*—Maps IP addresses to host names
- *NS (name server)*—Identifies other name servers for the domain

DNS Zone Transfer is typically used to replicate DNS data across a number of DNS servers, or to back up DNS files. A user or server will perform a specific zone transfer request from a "name server." If the name server allows zone transfers to occur, all the DNS names and IP addresses hosted by the name server will be returned in human-readable ASCII text.

3. How-to: DNS Enumeration Tools

In this tutorial I will cover some very basic methods on how to gather information about DNS on a specific target. We are using some tools to gather information about DNS. I will show you how to use DNSenum, Fierce, dig and host to gather DNS information from a domain.

DNSenum.pl

DNSenum is one of the tools that is used to gather as much information as possible about a domain. The program currently performs the following operations:

1) Get the host's addresses (A record).
2) Get the nameservers (threaded).
3) Get the MX record (threaded).
4) Perform axfr queries on nameservers (threaded).
5) Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").
6) Brute force subdomains from file can also perform recursion on subdomain that has NS records (all threaded).
7) Calculate C class domain network ranges and perform whois queries on them (threaded).
8) Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
9) Write to domain_ips.txt file ip-blocks.

By using this command, ***./dnsenum.pl --enum -f dns.txt --update a -r testsite.com,*** we can gather more information about the DNS records and DNS servers from an organization that we want to penetrate.

```
root@bt:/pentest/enumeration/dnsenum# ./dnsenum.pl --enum -f dns.txt --update a -r testsite.com
dnsenum.pl VERSION:1.2
Warning: can't load Net: Whois::IP module, whois queries disabled.
-----   testsite.com   -----
------------------
Host's addresses:
------------------
testsite.com.   38364   IN    A      172.20.201.17
testsite.com.   38364   IN    A      172.20.20.4
-------------
```

```
Name servers:
-------------
 ns1.dnsserver.com.      58099   IN     A      172.20.201.17
 testsite.com.  28109   IN     A      172.20.20.4
 testsite.com.  28109   IN     A      172.20.201.17
-----------
MX record:
-----------
 mail.testsite.com.     10133   IN     A      172.20.20.250
 posto.testsite.com.    38400   IN     A      172.20.20.7

----------------------
Trying Zonetransfers:
----------------------
 trying zonetransfer for testsite.com on ns1.dnsserver.com ...
 trying zonetransfer for testsite.com on testsite.com...
---------------------------------------------
Scraping testsite.com subdomains from google:
---------------------------------------------
 ----  Google search page: 1  ----
 www2
 ----  Google search page: 2  ----
 ----  Google search page: 3  ----
 ----  Google search page: 4  ----
 ----  Google search page: 5  ----
 ----  Google search page: 6  ----
 ----  Google search page: 7  ----
 ----  Google search page: 8  ----
 ----  Google search page: 9  ----
 Google results: 1
 Performing nslookups:
 www2.testsite.com.     10135   IN     A      172.20.20.30

------------------------------
Brute forcing with dns.txt:
------------------------------
 kawalan.testsite.com.   38400   IN     A      172.20.20.247
 atom.testsite.com.     38400   IN     A      172.20.20.94
 kawscent.testsite.com.     38400   IN     A      172.20.20.244
 kawscent2.testsite.com.      12397   IN     A      172.20.20.245
 hqserv.testsite.com.   38400   IN     A      172.20.20.154
 lmss.testsite.com.     38400   IN     A      172.20.20.193
 intranet1.testsite.com. 38400   IN     A      172.20.20.32
 kelam.testsite.com.    14237   IN     A      172.20.20.230
 kelam2.testsite.com.   38400   IN     A      172.20.20.232
 kedai2.testsite.com.   38400   IN     A      172.20.20.249
 linuxproxy.testsite.com.       38400   IN     A      172.20.20.3
 mail.testsite.com.     10126   IN     A      172.20.20.250
 server-ftp.testsite.com.       38400   IN     A      172.20.20.177
 marino.testsite.com.       38400   IN     A      172.20.20.97
 modeltest.testsite.com.    38400   IN     A      172.20.20.166
 nagios.testsite.com.   38400   IN     A      172.20.20.68
 montest.testsite.com.  38400   IN     A      172.20.20.77
 kosmos1.testsite.com.  38400   IN     A      172.20.20.151
 kosmos2.testsite.com.  38400   IN     A      172.20.20.152
```

office.testsite.com. 38400 IN A 172.20.20.195
posto.testsite.com. 38400 IN A 172.20.20.7
prass.testsite.com. 38400 IN A 172.20.20.95
radio.testsite.com. 38400 IN A 172.20.20.181
sms.testsite.com. 38400 IN A 172.20.20.20
webcam1.testsite.com. 38400 IN A 172.20.20.237
webcam2.testsite.com. 38400 IN A 172.20.20.238
windowsupdate.testsite.com. 38400 IN A 172.20.20.118
ssf.testsite.com. 38400 IN A 172.20.20.98
www.testsite.com. 10203 IN CNAME www2.testsite.com.
www2.testsite.com. 10203 IN A 172.20.20.30
www1.testsite.com. 38400 IN A 172.20.20.10
fileserver2.testsite.com. 38400 IN A 172.20.20.67

Performing recursion:

---- checking subdomains NS records ----
Can't perform recursion no NS records.
---
testsite.com c class netranges:

172.20.20.0/24
172.20.201.0/24

Performing reverse lookup on 512 ip addresses:
---
0 results out of 512 ip addresses.
---
testsite.com ip blocks:
---
done.
root@bt:/pentest/enumeration/dnsenum#

Fierce.pl

Fierce was created by Rsnake to address this very problem. Fierce tries multiple techniques to find all the IP addresses and hostnames used by a target. These include – trying to dump the SOA records, do a zone transfer, searching for commonly used domain names with a dictionary attack, adjacency scan and a couple of others.I will use fierce tool to find domain name information about the target host. This command will try to check whether domain can do zone transfer or not on the target host. Fierce found one domain name server and it will try to test for zone transfer allow. Nowadays, normally we could not find zone transfer enable on any domain because of security risk.

```
root@bt:/pentest/enumeration/fierce# ls
fierce.pl  hosts.txt
root@bt:/pentest/enumeration/fierce# ./fierce.pl -dns testsoft.com
DNS Servers for testsoft.com:
        mail.testsoft.com
Trying zone transfer first...
        Testing mail.testsoft.com
Whoah, it worked - misconfigured DNS server found:
testsoft.com. 38400   IN     SOA     testsoft.com. user.testsoft.com. (
                              1144471752      ; Serial
                              10800   ; Refresh
                              3600    ; Retry
                              604800  ; Expire
                              38400 ) ; Minimum TTL
testsoft.com. 38400   IN     NS      mail.testsoft.com.
testsoft.com. 38400   IN     MX      10 email.testsoft.com.
email.testsoft.com.   38400   IN     A       192.168.107.141
mail.testsoft.com.    38400   IN     A       192.168.107.141
web.testsoft.com.     38400   IN     A       192.168.0.2
www.testsoft.com.     38400   IN     A       192.168.107.141
Okay, trying the good old fashioned way... brute force
Checking for wildcard DNS...
Nope. Good.
Now performing 1896 test(s)...
192.168.107.141  email.testsoft.com
192.168.107.141  mail.testsoft.com
192.168.0.2      web.testsoft.com
192.168.107.141  www.testsoft.com
Subnets found (may want to probe here using nmap or unicornscan):
        192.168.0.0-255 : 1 hostnames found.
        192.168.107.0-255 : 3 hostnames found.
Done with Fierce scan: http://ha.ckers.org/fierce/
Found 4 entries.
Have a nice day.
```

From the results above, we found one misconfigured DNS server that allows performing zone transfer. We found SOA about that domain name. We found two interesting domain which is web.testsoft.com and mail.testsoft.com. From misconfigured DNS server, we can reveal a lot of information. We must understand that most of the DNS server disallow zone transfer on their domain. So what we need to do is to get host.txt file for the domain. Open host.txt file to check about sub domain and find interesting sub domain such as administrator, blog. There are a lot of functions in fierce.pl –h. One is –delay, -search and other function.

./fierce.pl -dns testsoft.com -search mail,webmail,web,www,admin

Host command

host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, **host** prints a short summary of its command line arguments and options.

name is the domain name that is to be looked up. It can also be a dotted-decimal IPv4 address or a colon-delimited IPv6 address, in which case **host** will by default perform a reverse lookup for that address. ***server*** is an optional argument which is either the name or IP address of the name server that **host** should query instead of the server or servers listed in */etc/resolv.conf*.

*root@bt:~# **host***
Usage: host [-aCdlriTwv] [-c class] [-N ndots] [-t type] [-W time]
[-R number] [-m flag] hostname [server]
-a is equivalent to -v -t ANY
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-i IP6.INT reverse lookups
-N changes the number of dots allowed before root lookup is done
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-v enables verbose output
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
-m set memory debugging flag (trace|record|usage)

This command will try to get or retrieves information about the name servers.

```
root@bt:~# host -t ns testsoft.com
testsoft.com name server mail.testsoft.com.
root@bt:~#
```

This command will try to perform a zone transfer by using the name servers found in the previous session.

```
root@bt:~# host -t ns sitecost.com
sitecost.com name server ns2.webtestsite.com.
sitecost.com name server ns1.webtestsite.com.
root@bt:~#
```

You can see that the transfer had been failed.

```
root@bt:~# host -l sitecost.com ns1.webtestsite.com
; Transfer failed.
Using domain server:
Name: ns1.webtestsite.com
Address: 192.168.163.157#53
Aliases:
Host sitecost.com not found: 5(REFUSED)
; Transfer failed.
root@bt:~#
```

You can see that the zone transfer had been successful.

```
root@bt:~# host -l testsoft.com mail.testsoft.com
Using domain server:
Name: mail.testsoft.com
Address: 192.168.107.141#53
Aliases:
testsoft.com name server mail.testsoft.com.
email.testsoft.com has address 192.168.107.141
mail.testsoft.com has address 192.168.107.141
web.testsoft.com has address 192.168.0.2
www.testsoft.com has address 192.168.107.141
root@bt:~#
```

Dig command

The command dig is a tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information. This tool can be used from any Linux (Unix) or Macintosh OS X operating system. The most typical use of dig is to simply query a single host.

```
root@bt:/pentest/enumeration# dig @mail.testsoft.com testsoft.com ns
; <<>> DiG 9.5.0-P2.1 <<>> @mail.testsoft.com testsoft.com ns
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20960
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;testsoft.com.                  IN      NS
;; ANSWER SECTION:
testsoft.com.       38400   IN      NS      mail.testsoft.com.
;; ADDITIONAL SECTION:
mail.testsoft.com.  38400   IN      A       192.168.107.141
;; Query time: 51 msec
;; SERVER: 192.168.107.141#53(192.168.107.141)
;; WHEN: Mon Apr 19 20:19:19 2010
;; MSG SIZE  rcvd: 67
```

This command shows that it will test for zone transfer:

```
root@bt:/pentest/enumeration/fierce# dig @mail.testsoft.com testsoft.com axfr
; <<>> DiG 9.5.0-P2.1 <<>> @mail.testsoft.com testsoft.com axfr
; (1 server found)
;; global options:  printcmd
testsoft.com.       38400   IN      SOA     testsoft.com. user.testsoft.com. 1144471752 10800 3600 604800 38400
testsoft.com.       38400   IN      NS      mail.testsoft.com.
testsoft.com.       38400   IN      MX      10 email.testsoft.com.
email.testsoft.com. 38400   IN      A       192.168.107.141
mail.testsoft.com.  38400   IN      A       192.168.107.141
web.testsoft.com.   38400   IN      A       192.168.0.2
www.testsoft.com.   38400   IN      A       192.168.107.141
testsoft.com.       38400   IN      SOA     testsoft.com. user.testsoft.com. 1144471752 10800 3600 604800 38400
;; Query time: 58 msec
;; SERVER: 192.168.107.141#53(192.168.107.141)
;; WHEN: Mon Apr 19 20:20:35 2010
;; XFR size: 8 records (messages 1, bytes 223)
root@bt:/pentest/enumeration#
```

4. Conclusion

DNS Server must configure securely to prevent attack to the DNS server. Without securing this feature of DNS, an attacker can easily obtain data from an organization's DNS servers. DNS holds a large amount of information about a domain, including server names and Internet Protocol (IP) addresses, services running on the network, and servers hosting specific services, such as global catalogs and domain controllers.

The accuracy of the results of DNS enumeration varies a lot depending on the Name Server being queried. A target network may have different domain name spaces that they employ and prior enumeration thru metadata, email headers and other methods reveal this domain names so as to be able to enumerate and take advantage of this service. Also a UDP and TCP portscan with fingerprinting is also a very good idea so as to find any NS server that might be part of a test system or internal exposed DNS server.

As a conclusion, there are a lot of open source tools available in the Internet that can be used to gather information about DNS. We must configure our DNS server securely to prevent attack from hackers or unauthorized users.

5. Reference

1. http://linux.about.com/library/cmd/blcmdl1_host.htm
2. http://en.wikipedia.org/wiki/Penetration_testing
3. http://www.inetdaemon.com/tools/host.shtml
4. http://www.securitytube.net/DNS-Zone-Transfers-with-Host-and-Dnsenum-video.aspx
5. http://docsrv.sco.com/NET_tcpip/dnsC.nslook.html
6. http://www.darknet.org.uk/tag/dns-enumeration/
7. http://en.wikipedia.org/wiki/List_of_DNS_record_types
8. Hacking Exposed Sixth Edition book.