4 Ways to DNS Enumeration

posted in PENETRATION TESTING on SEPTEMBER 1, 2017 by RAJ CHANDEL SHARE

Today we are going to perform DNS enumeration with Kali Linux platform only. It has in-built tool for DNS enumeration. For this tutorial you must be aware of DNS server and its records, if you are not much aware of DNS then read our previous article "**Setup DNS Penetration Testing Lab on Windows Server 2012**".

Nmap

Following command will try to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the responses.

The script first sends a query for _services._dns-sd._udp.local to get a list of services. It then sends a follow up query for each one to try to get more information.

nmap –script=broadcast-dns-service-discovery.

From given screenshot you can observe the running service on a DNS server.

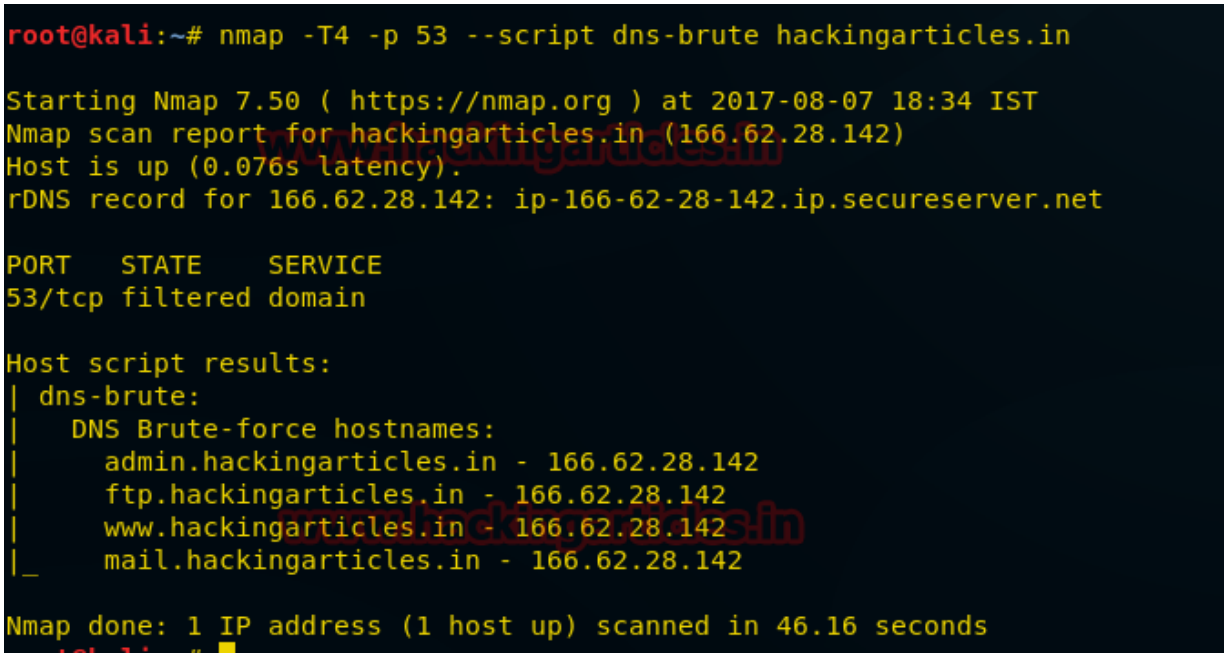
```
root@kali:~# nmap --script=broadcast-dns-service-discovery hackingarticles.in

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-07 17:48 IST
Nmap scan report for hackingarticles.in (166.62.28.142)
Host is up (0.060s latency).
rDNS record for 166.62.28.142: ip-166-62-28-142.ip.secureserver.net
Not shown: 982 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
25/tcp    open   smtp
26/tcp    closed rsftp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50500/tcp closed unknown
50800/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1276.60 seconds
```

Following command will try to enumerate DNS hostnames by brute force guessing of common subdomains. With the dns-brute.srvargument, dns-brute will also try to enumerate common DNS SRV records.

Wildcard records are listed as “*A” and “*AAAA” for IPv4 and IPv6 respectively.

nmap -T4-p 53 –script dns-brute www.hackingarticles.in

From screenshot you can observe DNs hostname



By default, the DNS server performs recursive queries on behalf of its DNS clients and DNS servers that have forwarded DNS client queries to it

Attackers can use recursion to deny the DNS Server service. Therefore, if a DNS server in your network is not intended to receive recursive queries, recursion should be disabled on that server

Following command will Checks if a DNS server allows queries for third-party names. It is expected that recursion will be enabled on your own internal nameservers.

From https://technet.microsoft.com

nmap -Pn -sU -p 53 –script=dns-recursion 192.168.1.150

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

As result you can observe that recursion is enable on targeted system

```
root@kali:~# nmap -Pn -sU -p 53 --script=dns-recursion 192.168.1.150

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-07 17:37 IST
Nmap scan report for 192.168.1.150
Host is up (0.012s latency).

PORT   STATE SERVICE
53/udp open  domain
| dns-recursion: Recursion appears to be enabled
MAC Address: 38:B1:DB:B3:BC:D9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

Following command will enumerates various common service (SRV) records for a given domain name. The service records contain the hostname, port and priority of servers for a given service. The following services are enumerated by the script: – Active Directory Global Catalog – Exchange Autodiscovery – Kerberos KDC Service – Kerberos Passwd Change Service – LDAP Servers – SIP Servers – XMPP S2S – XMPP C2S

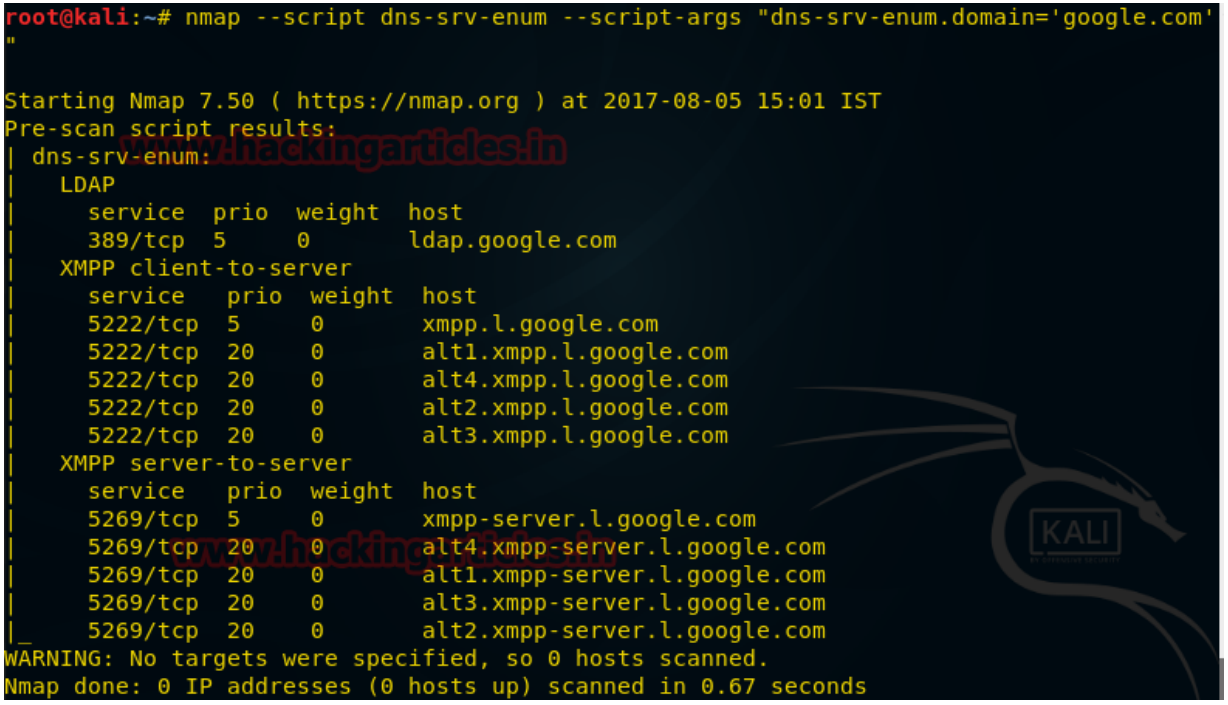
nmap –script dns-srv-enum –script-args “dns-srv-enum.domain=’google.com’

Articles

Select Month

Facebook Page

Be the first of your friends to like this



DNSEnum

Multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks.

OPERATIONS:

- Get the host's addresse (A record).
- Get the namservers (threaded).
- Get the MX record (threaded).
- Perform axfr queries on nameservers and get BIND VERSION (threaded).
- Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").

- Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
- Calculate C class domain network ranges and perform whois queries on them (threaded).
- Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
- Write to domain_ips.txt file ip-blocks.

Following command will avoid enumeration of reverse lookup and save the output result into xml format.

dnsenum –noreverse -o mydomain.xml hackingarticles.in

```
root@kali:~/Desktop# dnsenum --noreverse -o mydomain.xml hackingarticles.in
dnsenum.pl VERSION:1.2.3

-----   hackingarticles.in   -----


Host's addresses:
__________________

hackingarticles.in.                      28       IN    A        166.62.28.142


Name Servers:
______________

ns12.domaincontrol.com.                  172800   IN    A        208.109.255.6
ns11.domaincontrol.com.                  172800   IN    A        216.69.185.6


Mail (MX) Servers:
___________________

alt1.aspmx.l.google.com.                 177      IN    A        74.125.28.26
aspmx.l.google.com.                      171      IN    A        74.125.24.26
aspmx2.googlemail.com.                   230      IN    A        74.125.28.27


Trying Zone Transfers and getting Bind Versions:
________________________________________________


Trying Zone Transfer for hackingarticles.in on ns12.domaincontrol.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for hackingarticles.in on ns11.domaincontrol.com ...
AXFR record query failed: corrupt packet

brute force file not specified, bay.
```

DNSRecon

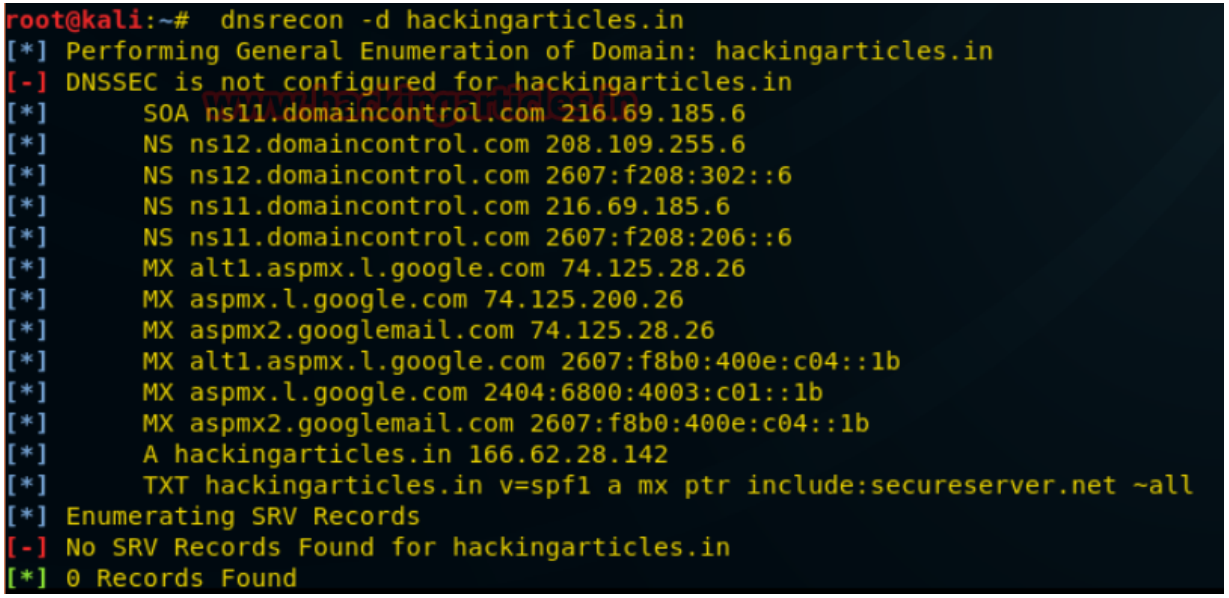
DNSRecon provides the ability to perform:

1. Check all NS Records for Zone Transfers
2. Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT)
3. Perform common SRV Record Enumeration. Top Level Domain (TLD) Expansion
4. Check for Wildcard Resolution
5. Brute Force subdomain and host A and AAAA records given a domain and a wordlist
6. Perform a PTR Record lookup for a given IP Range or CIDR
7. Check a DNS Server Cached records for A, AAAA and CNAME Records provided a list of host records in a text file to check
8. Enumerate Common mDNS records in the Local Network Enumerate Hosts and Subdomains using Google

Following command will enumerate DNS record of targeted website

dnsrecon-d hackingarticles.in

You can observe the result from given below image.



Fierce

Fierce is a reconnaissance tool. Fierce is a PERL script that quickly scans domains (usually in just a few minutes, assuming no network lag) using several tactics.

Type following command for DNS enumeration on targeted website

Fierce-dns hackingarticles.in

From screenshot you can see that we have scanned almost same result as from above tools.

```
root@kali:~# fierce -dns hackingarticles.in
DNS Servers for hackingarticles.in:
        ns12.domaincontrol.com
        ns11.domaincontrol.com

Trying zone transfer first...
        Testing ns12.domaincontrol.com
                Request timed out or transfer not allowed.
        Testing ns11.domaincontrol.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
166.62.28.142   admin.hackingarticles.in
166.62.28.142   ftp.hackingarticles.in
166.62.28.142   mail.hackingarticles.in

166.62.28.142   webmail.hackingarticles.in
166.62.28.142   www.hackingarticles.in

Subnets found (may want to probe here using nmap or unicornscan):
        166.62.28.0-255 : 5 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 5 entries.

Have a nice day.
root@kali:~#
```

Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST
← UNDERSTANDING LOG ANALYSIS OF WEB SERVER

NEXT POST
HACK THE 6DAYS VM (CTF CHALLENGE) →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

- [ ] Notify me of follow-up comments by email.
- [ ] Notify me of new posts by email.