

Experiment 04

Learning Objective:

To learn about DNS Enumeration & Reverse IP Lookup to extract the record to gather information about the websites.

Tools: MxToolbox and ViewDNS

Theory:

What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user's computer apart from the initial request.

Extracting Info from DNS Servers

Another way for pen testers to learn more about their targets is through DNS servers and records. DNS servers store a lot of useful information about their related networks, and there are a handful of tools to use for extracting valuable information about a target.

What DNS does (or, why we care)

DNS is part of the TCP/IP protocol suite. It's responsible for mapping user-friendly domain names (like "google.com") to an IP address (like "172.217.4.46").

A domain name server is a server with a large database of these mappings. For pen testers, accessing DNS servers provides them with a blueprint of the company's infrastructure, via a list of internal IP addresses and host names. As Engebretson notes in his book (The Basics of Hacking and Penetration Testing), DNS servers are often poorly configured or maintained, making them easy targets.

As always, only use this for legal purposes, with authorization, etc etc.

What is DNS Enumeration:

Finding every DNS server and its accompanying entries for an organization is known as DNS enumeration. A map or an address book is analogous to DNS.

The process of translating an IP address (192.111.1.120) to the name www.example.com and back is actually similar to that of a distributed database.

Before launching an attack, DNS enumeration is performed to learn as much as possible about your target. DNS servers can provide details about prospective target systems, like usernames, machine names, and IP addresses. To find a lot of data, DNS enumeration is performed. Numerous sorts of data related to a domain are frequently stored in the DNS system.

Tools: Tools required for Enumeration in DNS are MxToolbox, ViewDNS, nslookup, DNS Dumpster, and DNS recon.

What is Reverse IP Lookup?

Reverse IP lookup, also known as reverse DNS lookup, is the process of querying the Domain Name System (DNS) to determine the domain name associated with an Internet Protocol (IP) address.

Put in simpler terms, this tool looks up the owners of IP addresses (the numerical label assigned to devices on a network).

So, while your analytics software's IP tracking may tell you that your website has been visited by a user from IP address 73.50.51.77, reverse IP lookup can tell you that this visitor is from Acme Corporation. And yes, this is legal.

What Information Does Reverse IP Lookup Provide?

Tools that conduct reverse IP lookups provide top-level domain data associated with the IP. In most cases, you're getting the name of the business and sometimes the main phone number and address of those who registered the IP — not the specific name or contact info of the visitor.

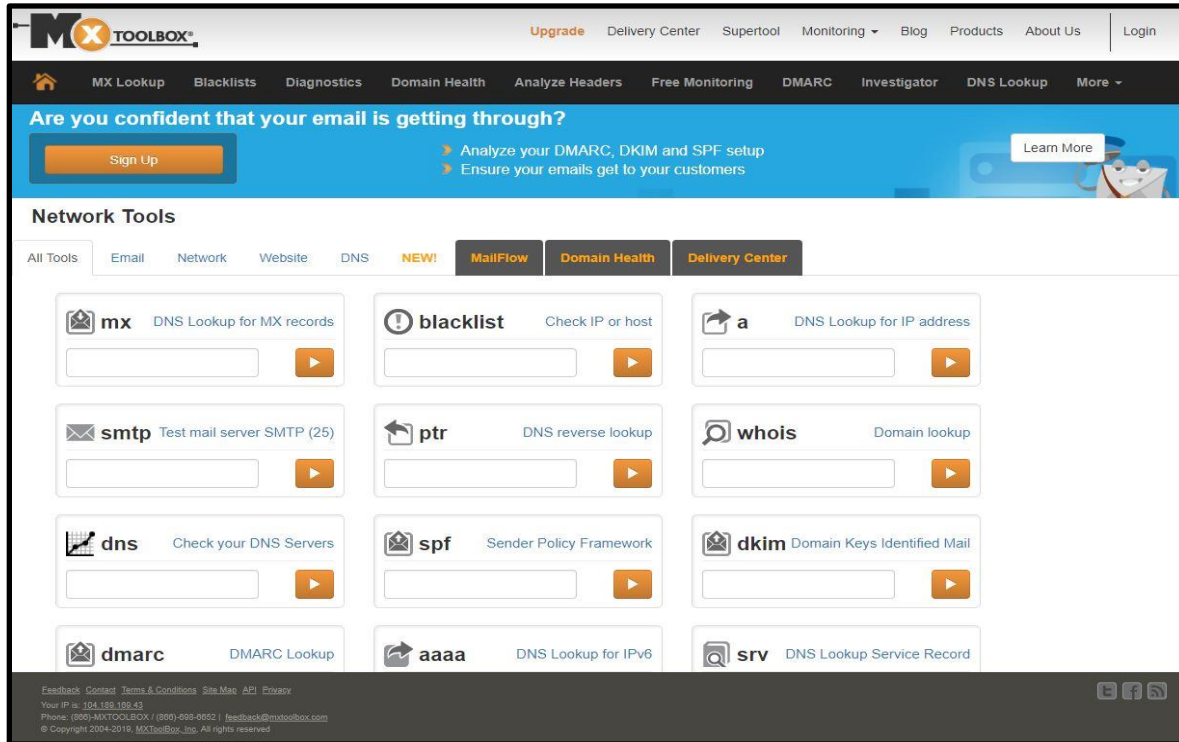
Reverse IP lookup tools pull information from databases that house IP information. These databases only carry public data and will only include static IP addresses tied to businesses or large networks. In other words, if someone visits your website from their home, it won't show a visit from "Bill McLastName"; instead, you'll see a visit from Comcast, Verizon, AT&T or whichever company provides Bill's internet.

Along with this information, reverse IP will also typically show you how many visits you received from the IP, how many visitors from this IP came to your site and when they visited.

What is the MXtoolbox?

MXtoolbox is an online set of tools and services designed to assist with the management and troubleshooting of email-related issues. It provides various diagnostic and monitoring tools specifically focused on email servers, DNS records, and email delivery. Best of all, it's free to use.

The primary purpose of MXtoolbox is to help administrators, IT professionals, and users identify and resolve issues related to email delivery, spam filtering, DNS configuration, and overall email server health.



Some of the key features and tools provided by MXtoolbox include:

1. **MX Lookup:**

This tool allows you to check the mail exchange (MX) records for a domain. Which specify the email server responsible for receiving emails for that domain.

2. **SPF Check:**

Sender Policy Framework (SPF) is a DNS record that helps prevent email spoofing. The SPF Check tool verifies if a domain's SPF record is properly configured.

3. **Blacklist Check:**

MXtoolbox can check if an IP address or domain is listed on various email blacklists, including Spamhaus, CBL, and others.

4. **SMTP Diagnostic:**

This tool performs a series of tests to diagnose issues with SMTP (Simple Mail Transfer Protocol) servers. Such as connectivity problems or SMTP authentication errors.

5. **Email Header Analyzer:**

This tool allows you to examine the headers of an email to gather information about its origin, route, and any potential issues.

6. DNS Lookup:

MXtoolbox provides a DNS Lookup tool to retrieve various DNS records for a domain, including A, CNAME, TXT, and MX records.

SuperTool Beta7

DNS Lookup

a:mxtoolbox.com
Find Problems
↻ a

Type	Domain Name	IP Address	TTL
A	mxtoolbox.com	13.32.208.14 <small>Amazon.com, Inc. (AS16509)</small>	60 sec
A	mxtoolbox.com	13.32.208.25 <small>Amazon.com, Inc. (AS16509)</small>	60 sec
A	mxtoolbox.com	13.32.208.57 <small>Amazon.com, Inc. (AS16509)</small>	60 sec
A	mxtoolbox.com	13.32.208.58 <small>Amazon.com, Inc. (AS16509)</small>	60 sec

Test	Result
✓ DNS Record Published	DNS Record found

Your DNS hosting provider is "Amazon Route 53" [Need Bulk Dns Provider Data?](#)

[dns check](#)
[mx lookup](#)
[dmarc lookup](#)
[spf lookup](#)
[dns propagation](#)
Reported by ns-1320.awsdns-37.org on 7/21/2023 at 4:55:32 AM (UTC -5). [just for you.](#)
[Transcript](#)

7. Email Deliverability:

This feature helps assess the deliverability of emails sent from a particular domain by performing tests and analyzing factors that can impact successful email delivery.

MXtoolbox is widely used by system administrators, email service providers, and anyone involved in managing email infrastructure. It offers a comprehensive set of tools to troubleshoot, analyze, and improve email-related issues, ensuring smooth email communication and enhancing the overall email server performance.

What is ViewDNS?

ViewDNS is an online tool to check DNS information and it is equally useful in many things. We will be using it for two main purposes:

1. Reverse Mail Exchange Lookup (Reverse MX Lookup)
2. IP History

Use of Reverse MX Lookup:

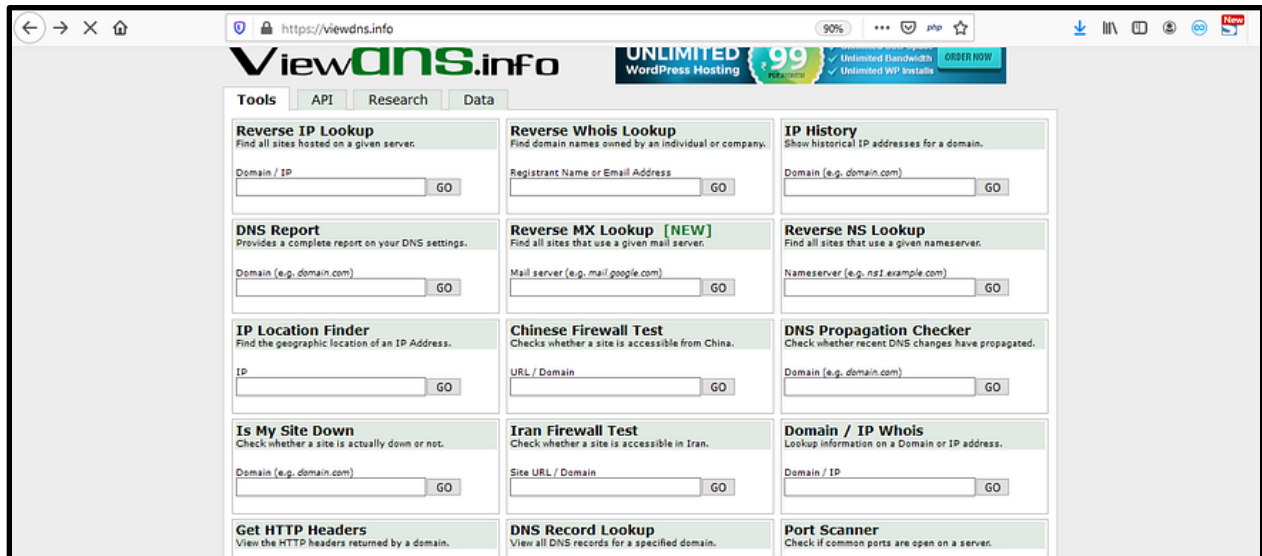
It takes a mail server (e.g., mail.google.com) and quickly shows all other domains that use the same mail server. Useful for identifying domains that are used as email aliases.

Use of IP History:

We will be using this feature to know how active our target website is because using IP History will show you the last seen of the particular IP address.

How to use ViewDNS for Reverse MX Lookup?

1. Go to <https://viewdns.info/> and you'll find many options



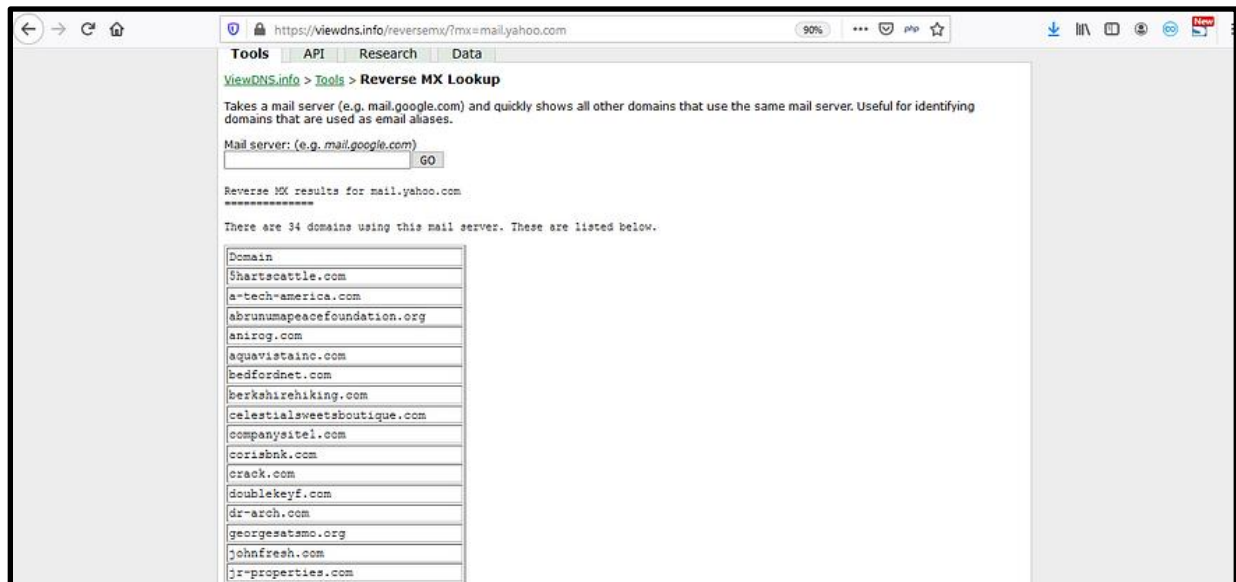
The screenshot shows the ViewDNS.info website interface. The browser address bar displays <https://viewdns.info/>. The website has a navigation bar with tabs for Tools, API, Research, and Data. A banner for 'UNLIMITED WordPress Hosting' is visible. The main content area features a grid of tool cards, each with a title, description, input field, and a 'GO' button:

- Reverse IP Lookup**: Find all sites hosted on a given server. Input: Domain / IP.
- Reverse Whois Lookup**: Find domain names owned by an individual or company. Input: Registrant Name or Email Address.
- IP History**: Show historical IP addresses for a domain. Input: Domain (e.g. domain.com).
- DNS Report**: Provides a complete report on your DNS settings. Input: Domain (e.g. domain.com).
- Reverse MX Lookup [NEW]**: Find all sites that use a given mail server. Input: Mail server (e.g. mail.google.com).
- Reverse NS Lookup**: Find all sites that use a given nameserver. Input: Nameserver (e.g. ns1.example.com).
- IP Location Finder**: Find the geographic location of an IP Address. Input: IP.
- Chinese Firewall Test**: Checks whether a site is accessible from China. Input: URL / Domain.
- DNS Propagation Checker**: Check whether recent DNS changes have propagated. Input: Domain (e.g. domain.com).
- Is My Site Down**: Check whether a site is actually down or not. Input: Domain (e.g. domain.com).
- Iran Firewall Test**: Check whether a site is accessible in Iran. Input: Site URL / Domain.
- Domain / IP Whois**: Lookup information on a Domain or IP address. Input: Domain / IP.
- Get HTTP Headers**: View the HTTP headers returned by a domain.
- DNS Record Lookup**: View all DNS records for a specified domain.
- Port Scanner**: Check if common ports are open on a server.

2. Enter your target IP or name in Reverse MX Lookup

Tools API Research Data		
Reverse IP Lookup Find all sites hosted on a given server. Domain / IP <input style="width: 100%;" type="text"/> <input type="button" value="GO"/>	Reverse Whois Lookup Find domain names owned by an individual or company. Registrant Name or Email Address <input style="width: 100%;" type="text"/> <input type="button" value="GO"/>	IP History Show historical IP addresses for a domain. Domain (e.g. domain.com) <input style="width: 100%;" type="text"/> <input type="button" value="GO"/>
DNS Report Provides a complete report on your DNS settings. Domain (e.g. domain.com) <input style="width: 100%;" type="text"/> <input type="button" value="GO"/>	Reverse MX Lookup [NEW] Find all sites that use a given mail server. Mail server (e.g. mail.google.com) <input style="width: 100%;" type="text" value="mail.yahoo.com"/> <input type="button" value="GO"/>	Reverse NS Lookup Find all sites that use a given nameserver. Nameserver (e.g. ns1.example.com) <input style="width: 100%;" type="text"/> <input type="button" value="GO"/>

3. Click on go and see the results



ViewDNS.info > Tools > Reverse MX Lookup

Takes a mail server (e.g. mail.google.com) and quickly shows all other domains that use the same mail server. Useful for identifying domains that are used as email aliases.

Mail server: (e.g. mail.google.com)


Reverse MX results for mail.yahoo.com

There are 34 domains using this mail server. These are listed below.

Domain
5hartsacattle.com
a-tech-america.com
abrunumapeacefoundation.org
anirog.com
aquavistainc.com
bedfordnet.com
berkshirehiking.com
celestialssweetsboutique.com
companystel.com
corisbkn.com
crack.com
doublekeyf.com
dr-arch.com
georgesatmo.org
johnfresh.com
jx-properties.com

How to use ViewDNS for IP History ?

1. Go to <https://viewdns.info/>
2. Enter your target IP or name in IP History



Tools | API | Research | Data

Reverse IP Lookup
Find all sites hosted on a given server.

Domain / IP

GO

Reverse Whois Lookup
Find domain names owned by an individual or company.

Registrant Name or Email Address

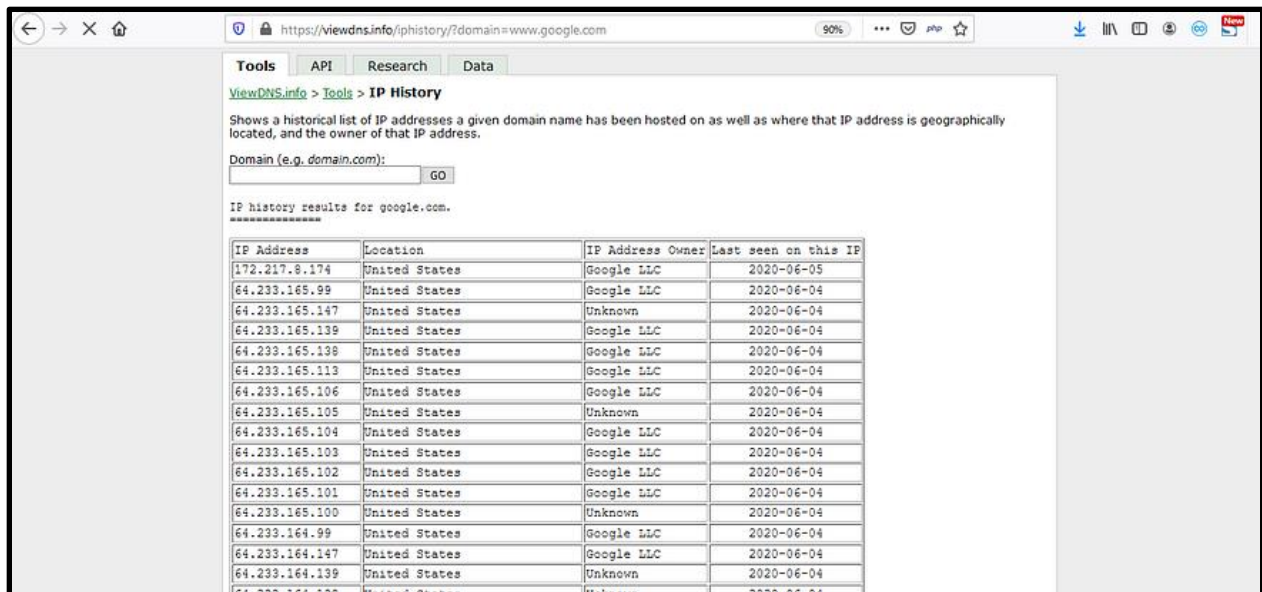
GO

IP History
Show historical IP addresses for a domain.

Domain (e.g. domain.com)

GO

3. Click on go and see the results



Tools | API | Research | Data

[ViewDNS.info](#) > [Tools](#) > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. domain.com): GO

IP history results for google.com.
 =====

IP Address	Location	IP Address Owner	Last seen on this IP
172.217.8.174	United States	Google LLC	2020-06-05
64.233.165.99	United States	Google LLC	2020-06-04
64.233.165.147	United States	Unknown	2020-06-04
64.233.165.139	United States	Google LLC	2020-06-04
64.233.165.138	United States	Google LLC	2020-06-04
64.233.165.113	United States	Google LLC	2020-06-04
64.233.165.106	United States	Google LLC	2020-06-04
64.233.165.105	United States	Unknown	2020-06-04
64.233.165.104	United States	Google LLC	2020-06-04
64.233.165.103	United States	Google LLC	2020-06-04
64.233.165.102	United States	Google LLC	2020-06-04
64.233.165.101	United States	Google LLC	2020-06-04
64.233.165.100	United States	Unknown	2020-06-04
64.233.164.99	United States	Google LLC	2020-06-04
64.233.164.147	United States	Google LLC	2020-06-04
64.233.164.139	United States	Unknown	2020-06-04
64.233.164.138	United States	Unknown	2020-06-04

Now we have the list of domains, subdomains, subdomains of subdomains, IP range, DNS information, domain registrar information etc. Now what to do for further recon? Let's see a new thing that this domains and subdomain communicates to which other external domains.

Learning Outcomes: The student should have the ability to

L01: Understand the concept of DNS Records

L02: How they can be used to perform information gathering about subdomains, mail servers, and other network resources

L03: How to use the MxToolbox and ViewDNS Tools for information gathering

Course Outcomes: Upon completion of the course students will be able to understand the concept of Extracting DNS Record to gather information and will be able to use MxToolbox and ViewDNS Tools for security purposes.

Conclusion: Through this experiment we learned the concept of DNS Enumeration & Reverse IP Lookup and we used the MxToolbox & ViewDNS to gather information.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				