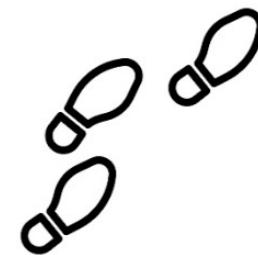


# What is Footprinting?

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.



Tribe Flood Network - Wikipedia

Wayback Machine

Leatt DBX 1.0 GripR Nero Glove

Internet Archive: Wayback Mach

https://web.archive.org/web/\*/google.com

Apps anime stuff XDCC 4chan gifs pdf D A B L study Araki Stuff aZP9X53\_700b.jpg (6 aqmvMVL\_700b\_v2.j Other bookmarks

ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE

SIGN IN

Search

INTERNET ARCHIVE

WaybackMachine

Explore more than 345 billion web pages saved over time

google.com

Find the Wayback Machine useful? [DONATE](#)

Saved 565,789 times between November 11, 1998 and January 10, 2019.

[Summary of google.com](#) · [Site Map of google.com](#)

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

JAN

FEB

MAR

APR

1 2 3 4 5

6 7 8 9 10 11 12

13 14 15 16 17 18 19

20 21 22 23 24 25 26

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

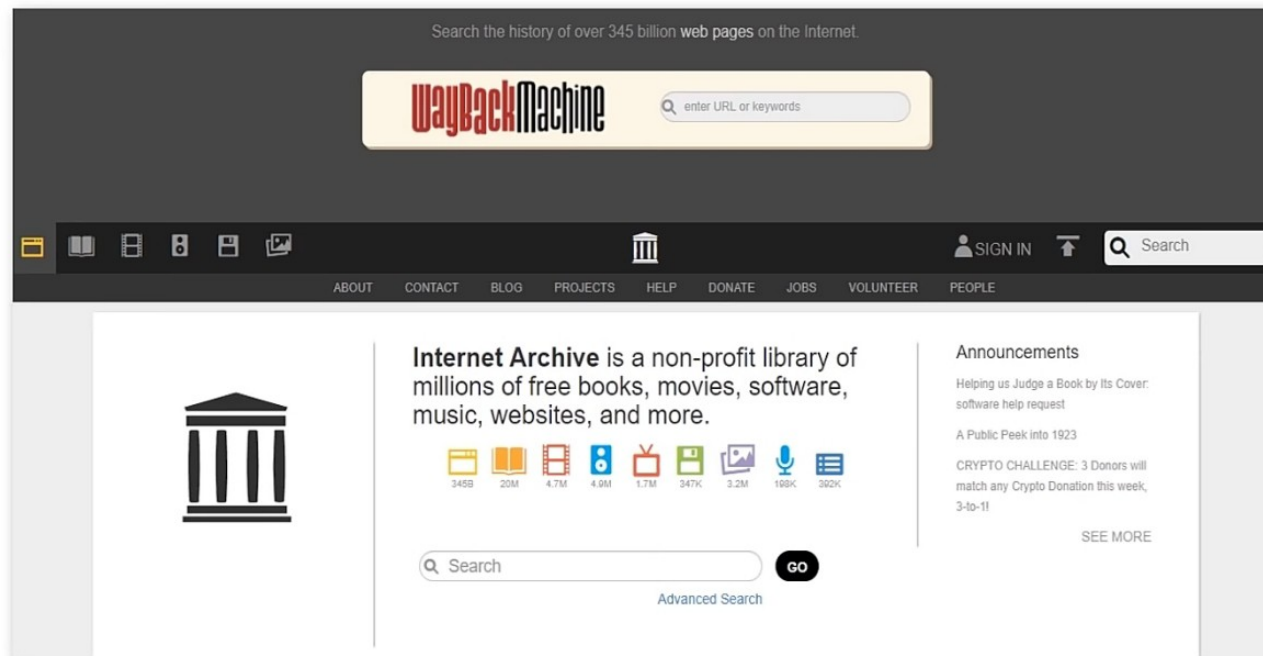
1 2 3 4 5 6

7 8 9 10 11 12 13

14 15 16 17 18 19 20

21 22 23 24 25 26 27


# Wayback Machine – Archive.org



Tribe Flood Network - WikipediGoogle! Search EngineLeatt DBX 1.0 GripR Nero GlovNetcraft | Internet ResearcherInstructor Led Online Courses

https://www.netcraft.com

Appsanime stuffXDCC4chan gifspdfAraki StuffaZP9X53\_700b.jpgaqmvMVL\_700b\_v2jOther bookmarks



Contact Us | Subscribe

HomeNewsAnti-PhishingSecurity TestingInternet Data MiningPerformanceAbout Netcraft

## Internet Security and Data Mining

Netcraft provide internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. We also analyse many aspects of the internet, including the market share of web servers, operating systems, hosting providers and SSL certificate authorities.


Anti-Phishing

Security Testing

Internet Data Mining

Performance


www.examplebank.com

  
Site Report

Risk rating: 0

Country: UKSite rank: 164,608

First seen: September 2000Host: Netcraft



Proactively defend your brand against phishing sites attempting to steal your users details:

- Over 56 million unique phishing sites blocked [January 2019]
- Third Party tests rate the Netcraft Toolbar as the most effective anti-phishing service
- Continuously updated feed suitable for network administrators, software developers and internet service providers
- Countermeasures service to eliminate fraudulent content on the internet
- Find out more

### Protect your customers


### Get in Touch

+44 (0) 1225 447500  
info@netcraft.com

### What's that site running?

Find out what technologies are powering any website:


### Audited by Netcraft

  
www.netcraft.com  
Security Audited 2019-01-10  
[Click to Verify](#)

This site is Audited by Netcraft. [Get your site scanned for vulnerabilities»](#)

### Report Suspicious URL

If you receive a phishing mail, please report the URL of the attacker's site.

SUBSCRIBE

ethical hacking:

1. active footprinting
2. passive footprinting

### **What is active footprinting?**

Active footprinting describes the process of using tools and techniques, like using the [traceroute](#) commands or a ping sweep -- [Internet Control Message Protocol sweep](#) -- to collect data about a specific target. This often triggers the target's intrusion detection system ([IDS](#)). It takes a certain level of stealth and creativity to evade detection successfully.

### **What is passive footprinting?**

As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using [Whois](#), a website that provides the domain names and associated networks for a specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.





## How do you start footprinting?

Reconnaissance is similar to footprinting and is a crucial part of the initial hacking exercise. It is a passive footprinting exercise where one collects data about the target's potential vulnerabilities and flaws to exploit while [penetration testing](#).

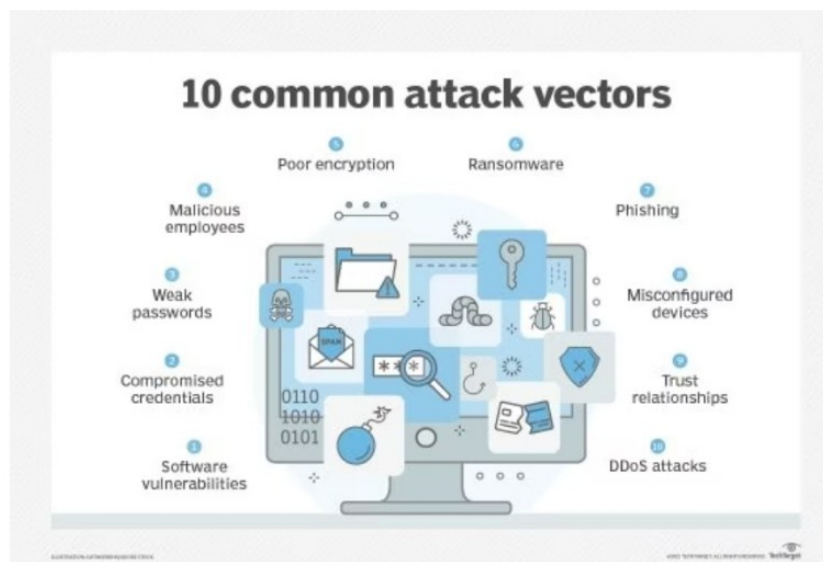
Security audits	Vulnerability assessments	Penetration testing
<ul style="list-style-type: none"><li>• Highly structured</li><li>• Policy vs. reality</li><li>• Business process reviews</li><li>• Determines whether controls exist</li><li>• References laws/security standards</li><li>• High-level tools are often used</li></ul>	<ul style="list-style-type: none"><li>• In-depth view</li><li>• Looks at technical flaws</li><li>• Scope is often external and internal systems</li><li>• Relies heavily on lots of good tools</li><li>• Typically doesn't include exploitation of weaknesses found</li><li>• Often confused with vulnerability "scans"</li></ul>	<ul style="list-style-type: none"><li>• Less structured</li><li>• Tightly-defined scope, typically external systems</li><li>• Sometimes operational flaws (i.e. social engineering) are included</li><li>• Time sensitive</li><li>• Relies heavily on limited set of good tools</li></ul>

Footprinting can help ethical hackers find potential vulnerabilities to assess and test.



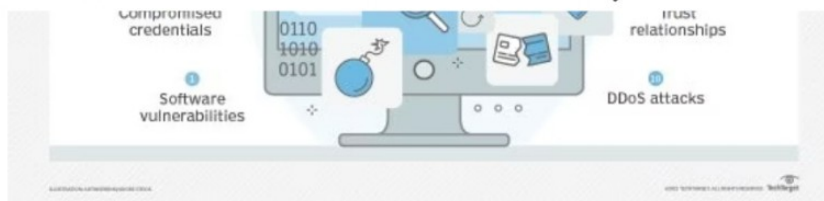
Footprinting processes start with determining the location and objective of an intrusion. Once ethical hackers identify a specific target, they gather information about the organization using nonintrusive methods, such as accessing the organization's own webpage, personnel directory or employee bios.

Ethical hackers collect this information and initiate [social engineering](#) campaigns to identify security vulnerabilities and achieve ethical hacking goals.



Footprinting is an excellent way to discover vulnerabilities to IT systems and infrastructure.

## Advantages of footprinting



Footprinting is an excellent way to discover vulnerabilities to IT systems and infrastructure.

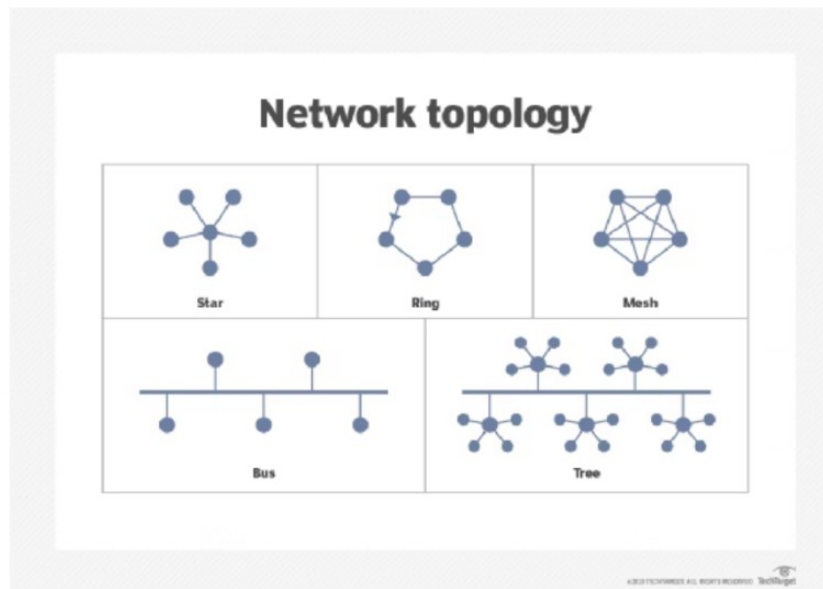
## Advantages of footprinting

Footprinting techniques in ethical hacking help businesses identify and secure IT infrastructure before a [threat actor](#) exploits a vulnerability. Users can also build a database of known vulnerabilities and loopholes.

Footprinting also helps companies better understand their current [security posture](#) through analysis of data gathered about the firewall, security configuration and more. Users can update this list periodically and use it as a reference point during security audits.

Drawing a network map helps cover all trusted [routers](#), servers and other [network topologies](#). Users can pursue a reduced attack surface by narrowing it down to a specific range of systems.





Drawing network maps of trusted network topologies, including routers and servers, as part of a footprinting exercise is a good way to reduce attack surfaces.

## Other types of footprinting

**DNA footprinting** is the method used to identify the nucleic acid sequence that binds with proteins.

An **ecological footprint** is an approach to measuring human demand for natural capital or resources. It calculates the amount of natural resources required to support people or an economy. Ecological footprinting uses an ecological accounting system to keep track of this demand.

A **digital footprint** describes one's unique, traceable digital activities.



**DNA footprinting** is the method used to identify the nucleic acid sequence that binds with proteins.

An **ecological footprint** is an approach to measuring human demand for natural capital or resources. It calculates the amount of natural resources required to support people or an economy. Ecological footprinting uses an ecological accounting system to keep track of this demand.

A **digital footprint** describes one's unique, traceable digital activities. These include actions, communications and contributions expressed on the internet or digital services. Digital footprints can be either active or passive.



Explore the [future of cybersecurity](#), and