



CODE-EPIC

Code Epic Technologies

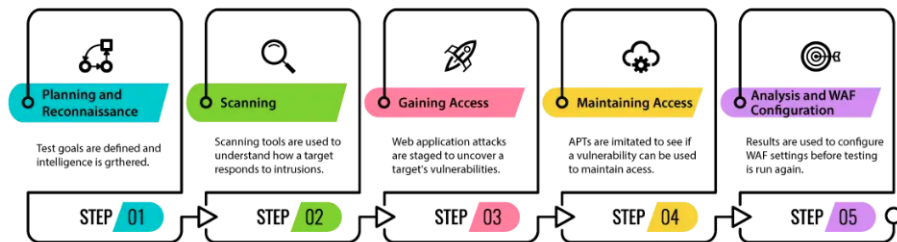
PLANNING AND RECONNAISSANCE

Surviving technology

cr4sh.m4d0v3r

<https://code-epic.github.io>

June 2022



1 Phase 1

The first penetration step involves planning to simulate a malicious attack – the attack is designed in a way that helps to gather as much information on the system as possible.

This is possibly one of the most time-consuming stages as ethical hackers inspect the system, note the vulnerabilities, and how the organization's tech stack reacts to system breaches. The information searched ranges from names and email addresses of the company's employees to network topology, IP addresses, among others. It should be noted that the type of information or the depth of the investigation will depend on the objectives set for the audit. Some gathering methodologies include social engineering, dumpster diving, network scanning, and domain registration information retrieval.

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below

1. Gather initial information
2. Determine the network range
3. Identify active machines
4. Discover open ports and access points
5. Fingerprint the operating system

6. Uncover services on ports
7. Map the network

We will discuss in detail all these steps in the subsequent chapters of this tutorial. Reconnaissance takes place in two parts - Active Reconnaissance and Passive Reconnaissance.

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

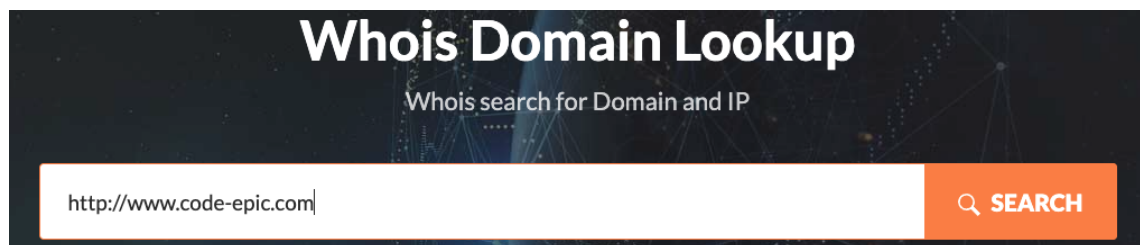
In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

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. Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target. During this phase, a hacker can collect the following information

1. Domain name
2. IP Addresses
3. Namespaces
4. Employee information


5. Phone numbers
6. E-mails
7. Job Information

In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet. Domain Name Information You can use <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.


A screenshot of a 'Whois Domain Lookup' web interface. The title 'Whois Domain Lookup' is in large white font on a dark background. Below it, the subtitle 'Whois search for Domain and IP' is in smaller white font. A search input field contains the text 'http://www.code-epic.com'. To the right of the input field is an orange button with a magnifying glass icon and the word 'SEARCH' in white capital letters.

Whois Domain Lookup

Whois search for Domain and IP

 **SEARCH**

Here is sample record of www.code-epic.com extract from WHOIS Lookup

 Registrant Contact	
Organization:	Privacy service provided by Withheld for Privacy ehf
Street:	Kalkofnsvegur 2
City:	Reykjavik
State:	Capital Region
Postal Code:	101
Country:	IS
Phone:	+354.4212434
Email:	7659dd630d2e4b4c9113edd5857865dc.protect@withheldforprivacy.com

How Does Ping Work?

Ping comes from a term used in sonar technology that sends out pulses of sound, and then listens for the echo to return. On a computer network, a

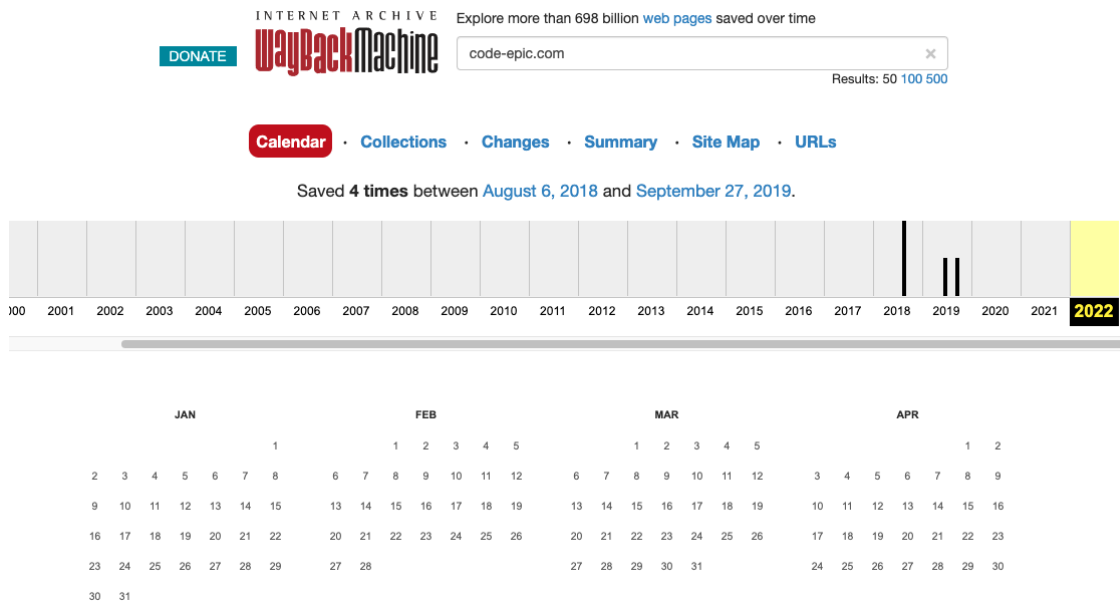
ping tool is built into most operating systems that works in much the same way. You issue the ping command along with a specific URL or IP address. Your computer sends several packets of information out to that device, and then waits for a response. When it gets the response, the ping tool shows you how long each packet took to make the round trip or tells you there was no reply.

```
> ping -c 1 code-epic.com
PING code-epic.com (172.67.162.169): 56 data bytes
64 bytes from 172.67.162.169: icmp_seq=0 ttl=52 time=76.800 ms

--- code-epic.com ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 76.800/76.800/76.800/0.000 ms
```

History of the Website?

It is very easy to get a complete history of any website using <http://www.archive.org>. You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.



Quick Fix?

Though there are some advantages of keeping your website in an archive database, but if you do not like anybody to see how your website progressed through different stages, then you can request archive.org to delete the history of your website.

Nmap ("Network Mapper")

Is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping)

```
> nmap -p443 -T5 -vvv -n -Pn 65.108.62.7
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-13 22:36 -04
Initiating Connect Scan at 22:36
Scanning 65.108.62.7 [1 port]
Discovered open port 443/tcp on 65.108.62.7
Completed Connect Scan at 22:36, 0.20s elapsed (1 total ports)
Nmap scan report for 65.108.62.7
Host is up, received user-set (0.20s latency).
Scanned at 2022-06-13 22:36:27 -04 for 0s

PORT      STATE SERVICE REASON
443/tcp   open  https  syn-ack

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

2 Recommendation

I share videos and concepts for the recognition of a domain or equipment.

Penetretaiion Testing

<https://www.youtube.com/watch?v=4Zn6qgqxmWY>

<https://www.youtube.com/watch?v=ZqjTVvDY7GY>

Icann Seven Keys

Seven Key Internet To protect DNS, ICANN came up with a way of securing it without entrusting too much control to any one person. It selected seven people as key holders and gave each one an actual key to the internet. It selected seven more people as backup key holders Nmap.org has been re-designed! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.

<https://www.youtube.com/watch?v=B-icPvF3RG8>

<https://www.youtube.com/watch?v=YlLo6Man4iE>