Network Penetration Testing-Part 1

Piyush Patil
May 17 · 4 min read ★

Penetration testing (or pen testing) is a security exercise where a cyber-security expert

4. Maintaining Access/ Post-exploitation

5. Covering Tracks

. . .

> *Lets start with: Information Gathering*

Our aim is to collect information about the following things:-

Network Architecture, Network Blocks, IP addresses, Open Ports, Services and Applications, Web server (Version, DNS info), OS information and any other available devices information, Email addresses, Any document which will contain useful information.

> *Two types of information gathering*

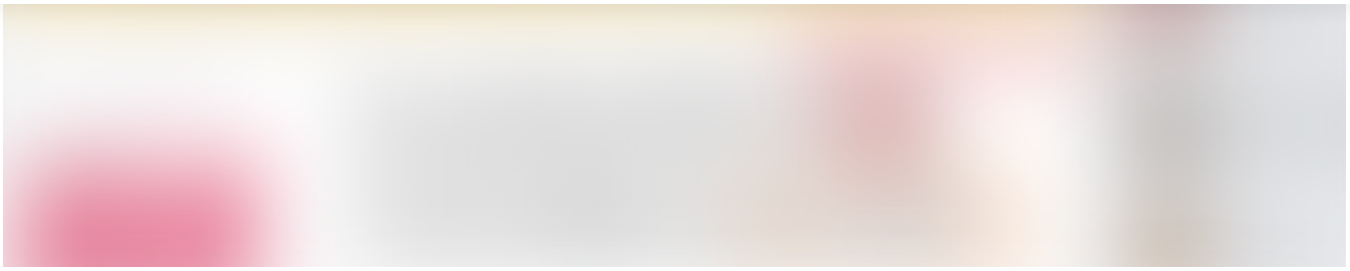
Active — We interact directly with the target system

Passive-We don't interact directly with the target system

. . .

> *Google Dorking*

Google Dorking means using google with some keyword to collect target information.



site — will return website on following domain

intitle — contains title specified phrase on the page

inurl — restricts the results contained in the URLS of the specified phrase

filetype — search for specified filetype formats

We can also mix above dorks:-

site:pdfdrive.com filetype:pdf

Finding Subdomains

site:google.com -site:www.google.com

. . .

> *Whois*

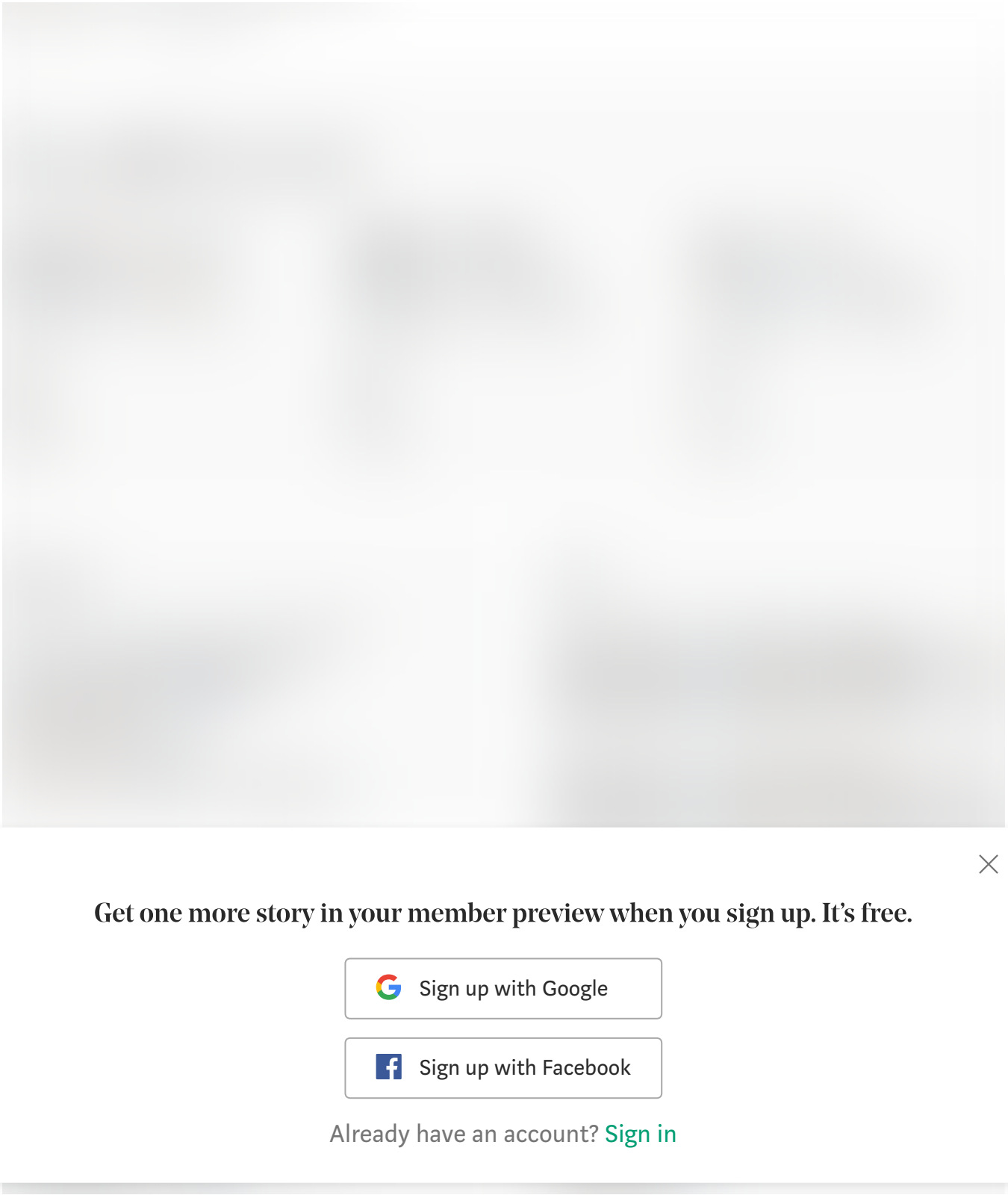
Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them.

- IP history

There are two ways to use whois.

1.By using website

https://whois.icann.org/en



2-By using tool (preinstalled in most of the Linux)

whois google.com

. . .

> *Wayback Machine*

If we want to see cached or archive site, visit https://archive.org/web/

It will ask you for the name of the website and select a date. In my case, I want to see how Google was in 1998.

. . .

python3 -m pip install -r requirements.txt

./theHarvester.py -d wipro.com -b google

-d =>domain name of company

-b => search engine

List of available search engines:-

https://github.com/laramies/theHarvester

. . .

DNS Enumeration

There are so many different ways and tools to get this information. But I prefer dnsenum which gives us information about:

Name servers

Mail servers

Tries DNS zone transfer

Installation:

apt-get install build-essential

git clone https://github.com/fwaeytens/dnsenum

install Net::Netmask

cd dnsenum

./dnsenum.pl google.com

. . .

Metagoofil

Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Installation

apt-get install metagoofil

Metagoofil -d anywebsitename.com -t pdf -l 100 -n 50 -o /root/Home -f output.html

-d: domain to search

-t: filetype to download (pdf, doc,xls,ppt, odp, ods, docx,xlsx, pptx)

-l: limit of results to search (default 200)

-h: work with documents in directory (use “yes” for local analysis)

-n: limit of files to download

-o: working directory (location to save downloaded files) -f: output file

Linkedin — Job Openings with their requirement, Employment history, and skills

Twitter — Controversial (?) personal views

Google+ — Pattern of life, friend circle

. . .

> *Shodan*

Shodan is a search engine for finding specific devices, and device types, that exist online. The most popular searches are for things like webcam, Linksys, Cisco, Netgear, SCADA, etc.

Here are the basic search filters you can use:

- **city**: find devices in a particular city
- **country**: find devices in a particular country
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on the operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

country:”FR”

geo:

Find devices by giving geographical coordinates.

geo:”21.452673,56.245212"

hostname:

Find devices matching the hostname.

server: “gws” hostname:”google”

net:

Find devices based on an IP address or /x CIDR.

net:210.214.0.0/16

os:

Find devices based on operating system.

os:”windows 10"

port:

Find devices based on open ports.

Port:22

WRITTEN BY

Piyush Patil

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Follow

More From Medium

Also tagged Risk

Salome Balderrama in CLIMURGENCY
Dec 4 · 7 min read ★

38

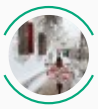
Top on Medium

Do They All Want To Sleep With Me? — And Other Questions Of A Guys' Girl

Tesia Blake in P.S. I Love You
Nov 21 · 7 min read ★

2.9K

Apparently I Was Nothing But A Woo-Girl



Michelle Ann in Fearless She Wrote
Nov 13 · 4 min read ★

4.8K