What Ethical Hackers / Pentester looking for ?

Network Information

> Domain Names
> Internal Domains
> IP Addresses
> Unmonitored / Private Websites
> TCP / UDP Services
> VPN / IDS / IPS / Acces Controls
> VPN Info
> Phone Numbers / VoIP

Operating System Information

> User & group names / info
> Banner grabbing
> Routing tables
> SNMP
> System architecture
> Remote System
> System Names
> Passwords

Organization Information

> Organization Website
> Company Directory
> Employee Details
> Location Details
> Addresses / Phone Numbers
> Comments in HTML Source Code
> Security Policies Deployed
> Web Server Links
> Background of Organization
> News / Press Release

Types of Reconnaissance

> Passive Reconnaissance

> Active Reconnaissance

External / Passive Reconnaissance
> Network (IP addresses and Domain Name)
> Phone
> Website
> Source Code
> Website Mirroring
> Archive Sites
> github recon
> Whois
> Web Servar Content
> Email Header
> Google and Search Engine
> Google Hacking
> People Sites
> Social Networks
> Job Sites
> Alert Websites

Internal / Active Reconnaissance
> IP addresses
> Internal DNS
> Private Websites
> Dumpster Diving
> Shoulder Surfing
> Eavesdropping

Website information

> Employee details (User Name / Email)
> Location details
> Addresses
> Phone numbers

create a list of User Name, Email, Addresses, Phone numbers, Location details and some sensitive information also.

A sitemap is a file where you provide information about the pages, videos, and other files on your site, and the relationships between them.

One by one visit the sitemap urls and see is there any sencetive information axsist or not. By using sitemap we know how many url's we visited or how many url's is remaining for visit. All website's not contains sitemap but Most of the website's contains sitemap. sitemap is placed For Search engin's .

Types of sitemap:
> user sitemap - sitemap.html - user index
> Search engin sitemap - sitemap.xml

User sitemap is available on the footer of the website, make for users.
(example:- https://example.com)

Search ingen sitemap is made for search engines. This is the search engine index. (example:- https://www.example.com/sitemap.xml)

If sitemap is not available on the website then we will generate the sitemap. By Using this website (https://www.xml-sitemaps.com/) we can create sitemap.html and sitemap.xml file for any website.

sitemap.xml vulnerability hackerone:- https://hackerone.com/reports/318603

robots.txt
In robots.txt file here is some links which is not for users, as well as not visible for users and which is not allowd to index by search engine.

> robots.txt - Disallow for any user agent and google / search engine

https://wwwexample.com/robots.txt

Extract all anker tag of the perticular page. we get all anker tag links by this.
(download the output in csv or excel both format.)

https://www.convertcsv.com/url-extractor.htm

screamingfrog
SEO Spider, do indexing like search engines, this goes to website and how many contents or pages are there and generate index then provide us output. the functonality of this tool is goes one link to second link and second link to third link this is called spider. user friendly .output. internal links and external links all link is shown in output

> seo spider - https://www.screamingfrog.co.uk/seo-spider/

Mirror the website
Mirror the website For analysing web pages source code.

> Locally mirroring the website - Read Source Code

wget
wget -m https://example.com

HTTrack
HTTrack availabe on both windows or kali linux (GUI or CLI both) (alternative option for Mirroring)

httrack https://example.com

Waybackmachine
Previous content identify. May be we get some sensitive information and end points like user name and all those thing.
archive is a collection of usefull information or historical documents or records providing information about a place, institution, or group of people.
For this we use two resources:

> Waybackmachine - https://archive.org
> archive.today - https://archive.ph/

https://archive.org take a snapshot of website. save website look and feel frontend html, css, javascript and store. and old resource also available. websites, books, software and so on. to see old version of website go to https://archive.org waybackmachine enter the url https://example.com Click on Brows History.

we can archive website content by using https://archive.ph/ go to https://archive.ph/ here (My url is alive and I want to archive its content) enter the url of the website which we want to archive https://example.com the click to save.

to see old version of website go to https://archive.ph/ here (I want to search the archive for saved snapshots) enter the url of the website https://example.com then click to search.

waybackurls
It is use for find out end points, end point it means url. waybackurls give us numbers of url. All those number of Resources that have now been removed, The page that used to be before that is now deleted.we can see that pages by using waybackmachine but here we want the urls of the deleted pages. for web pages content we use waybackmachine and for page urls we will use Waybackurls.

For waybackurls we must have install golang.

apt install golang

create a directory in which we will clone the git reposetory.

mkdir -p /root/go/bin
cd /root/go/bin

Now clone the git reposetory by using go command.

go get github.com/tomnomnom/waybackurls

Now we have waybackurls binary file. we will put this binary file to /usr/local/bin/ for run this binary from anywhere.

cp -v /root/go/bin/waybackurls /usr/local/bin/
waybackurls --help

The waybackurls command is working. Now we give a url to waybackurls command.

waybackurls https://www.example.com

Now we have numbers of previous waybackurls. May be this url's or nubers of resource or link also exist today, which is removed from the website.
By using waybackurls we get the end points or link or url of the target.

this file tell about technology use.
>	readme.html or readme.txt

https://example.com/readme.html
https://example.com/readme.txt

what technology are used for website some information may be
(also see this files and folder).

https://example.com/crossdomain.xml
https://example.com/clientaccesspolicy.xml
https://example.com/license.txt
https://example.com/.well-known
https://example.com/feed

On what technology is the website built?

>	readme.html
>	readme.txt
>	licence.txt
>	feed (RSS feed)

we get some information in these files which through we can ensure that on what technology is the website built.

Other than this, there are some other online resources that we use.
like:

> https://builtwith.com/
> https://www.wappalyzer.com/

builtwith and wappalyzer analyze source code of the frontend language of the website, and tell us that on what technology is the website built or what methology is use.
builtwith and wappalyzer addon also available.

whatweb https://example.com/

whatweb http://192.168.1.40

Verifying information from more than one place is the right approach.

siteinfo
Website Traffic, Statistics, and Analytics related information

alexa

> https://www.alexa.com/

> https://www.alexa.com/siteinfo

> https://www.alexa.com/topsites

we get site traffic, global rank related information and so on.

whois
Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them.
The Ferst step visit all website urls, then Note down the contact information, person / user names, email and other information.
while visiting website another than this some external links and social networking websites / media platform links if axist note down that also. if organization have any other websites that is not link wth and that websites also belong to these organization then to find them and for other details of the website we use whois.

email, user name, address, domain name, managed name server name, registrar name, contact no., when domain register, when domain expire this all details stores whois, before this all information was publicly available, but now some details is publicly available and some details removed from publicly available and moved to privately available.

Registrant name, Name server, Email, phone number,

whois example.com
> https://www.whois.com
> https://who.is
> https://in.godaddy.com/whois
> https://www.whoxy.com/
> https://viewdns.info/whois/

search the website details in whois database and get some information like ;

whois of the domain name:

Domain Name:
Registry Domain ID:
Registrar WHOIS Server:
Registrar:
Registrar URL:
Creation Date:
Updated Date:
Registrar Registration Expiration Date:
Registrant State/Province:
Registrant Country:
Name Server:

whois of the ip:

 if you have ip its ok, if you not have ip you have domain name then get ip of the domain by resolving dns query.

dig example.com

  now we get ip of the domain name, now search this ip in whois database if the given ip whois recrd exist than we will definetly get the whois information.

  if whois not give any info of the given ip then try ip to location.

  Verifying whois information from more than one place is the right approach, and by this we can get some other (diffrent) and more details.

By visit website or by whois search we have some email, contact no., username. behalf of this information we will find how many domains register by this email and contact no., corresponding we will know how many domain link to each other. here we will use reverse whois.

reverse whois
 whatever email or name we have, we will utilaize that here. behalf of given email or name here we get some information, about how many domain registered with email or name.

> https://viewdns.info/reversewhois/
> https://www.reversewhois.io/
> https://www.whoxy.com/reverse-whois

 we get here some domain list related to the given name or email.

 some detail we get from whois and some detail we get from reverse whois and some detail we get from website external link. how many numbers of domain we get, we should make a list of.

 we know that websites run by domain name or ip both, then first we will hit by domain name and check what is running there, then we will translate domain to ip by resolving dns query, then hit on ip and check what is running there.

> # dig example.com
(translate domain to ip)
> # dig +short example.com
or
> # dig -f domain.list
> # dig -f domain.list +short > ip.output
create a list of domains and ip. And then the our next approch will be by ip.

when we hit on ip may be we get same website or may be different website or may be we get server page (or difault page).

now we will find out whether the ip belongs to a server or is a share hosting, also we will find that what is the physical address (isp) of the ip or what type of hosting use on the ip. by using ip to location.

ip to location
ip to location will tell us where the server exists. Here we will know Who has taken the ip on lease and who is the isp (internet service provider).

> https://www.iplocation.net/
> https://iplocation.com
> https://ipinfo.io/
> https://tools.keycdn.com/geo

Here we understand by isp that server is self hosted or share hosting. is isp provide any share hosting services / CDN or not, by analysing isp detail we understand that what is the type of hosting, self hosted or not.

our first approch is data not website. data is store on internal server / network. if we not able to get any data than, after that we can compromise with website, and than we approch to services down on website. but our main aim is data, not website.

Here we define that what type of data breach we want internal server / network, or website.

Here we define that where / what is our target. server / network or website.

if we get any self hosted server, by analysing isp detail, than we will go for next approach.

now we know that where we will get the ip of server / network, but still we miss some thing. till now we dont get all ip, we have some ip till now. for more ip finding we will use some more approch.

domain to ip
find some more ip by resolving dns query

> # dig +short example.com
> # dig +short example.com ns
> # dig +short example.com mx
> # dig +short ns1.exampledns.com
> # dig +short ns1.exampledns.com
> # dig +short mx.examplemail.com
> # dig +short mx.examplemail.com
> # dig +short example.com any
> # dig - f domain.list
> # dig - f domain.list +short > ip.output

(if we get any record of the domain so save it. some time we get some info by any record.)

Now make a list of all ip which we have.
Read:- What services are use within a corporate network / servers?

Now we will use some more resourses to find ip by using below givan tools.

Google Admin Toolbox Dig
put here domain name and we will get some dns record details.

> https://toolbox.googleapps.com/apps/dig/

similar google Public DNS

> https://dns.google/

same ViewDNS.info > Tools > DNS Report
put her domain name we get here all dns record resolve and some more information.

> https://viewdns.info/dnsreport/

ViewDNS.info > Tools > DNS Record Lookup
put her domain name we get here all dns record resolve

> https://viewdns.info/dnsrecord/

> https://www.ultratools.com/tools/dnslookup/

centralops.net
put her domain name we get here domain to ip and all dns record resolve and also whois data, traceroute, network whois record and service scan.

> https://centralops.net/co/

DNStools
put her domain name we get here all dns record resolve

> http://en.dnstools.ch/dns-nameserver.html
> https://www.robtex.com/dns-lookup/

viewdns.info website we want to complitly view, here the no. of option is more useful, and this is more usefull.

https://viewdns.info/

ip history
all the previous ip of the domain
https://viewdns.info/iphistory/

how many websites are run wit given domain on hosting server, how many websites are running by given ip.

https://viewdns.info/reverseip/

dns record resolver
https://viewdns.info/dnsreport/
https://viewdns.info/dnsrecord/

reversewhois
how domains are running by domain

https://viewdns.info/reversewhois/

mail server look up we get here mail server details. how many numbers of user (domain) use this mail server service.

dig +short example.com mx

https://viewdns.info/reversemx/

ViewDNS.info > Tools > Reverse NS Lookup
we get here how many domain use the given nameserver

dig +short example.com ns
https://viewdns.info/reversens/

chacking how many port is enable. how many no. of port is enable on the given domain / server by this we can make connection or comunicate to server or domain. when ids / ips empliment on the server when we use this website. if ids / ips empliment on the server when website ip block not our ip, if we use this url.

https://viewdns.info/portscan/

yougetsignal
give here domain ip to find how many port is enable

> https://www.yougetsignal.com/tools/open-ports/

> http://en.dnstools.ch/port-scan.html

if we get open port details then brows the services and verify that services. and note down the open services port details.

Read:- What services are use within a corporate network / servers?

Traceroute
find how many no. of nodes are axists between the target and us.

traceroute target ip

IP Traceroute Tool

traceroute 8.8.8.8

traceroute 2404:6800:4009:815::200e

tracepath 8.8.8.8

tracepath 2404:6800:4009:815::200e

C:/> tracert 8.8.8.8

https://viewdns.info/traceroute/

tracepath
same find how many no. of nodes are axists between the target and us.

apt install iputils-tracepath
tracepath target ip
tracepath target ipv6

https://viewdns.info/traceroute/

Now make a list of all ip which we have with ther services.
now we have some more information of the target.

IP Address History

IP Address History

https://viewdns.info/iphistory/

all the previous ip of the domain

Reverse IP Add Domain Lookup

Reverse IP Domain Lookup

https://www.yougetsignal.com/tools/web-sites-on-web-server/

Reverse Mail Server Lookup

Reverse Mail Server Lookup

dig example.com mx

nslookup -type=mx example.com

https://viewdns.info/reversemx/

Reverse Nameserver Lookup

Reverse Name Server Lookup

dig example.com ns

nslookup -type=ns example.com

https://viewdns.info/reversens/

Open Ports Check

Open Ports Check

https://viewdns.info/portscan/

https://www.yougetsignal.com/tools/open-ports/

Google Hacking Database

Google Hacking
Google is a worldwide recognize search engine which user spattering technique to search a specific query.
There are so many search engines are there example: - AOL, A9, DOG PILC, Bing and Yahoo search.
Google offers special terms known as operators to help you perform more advanced queries. These
Operators help you to get exactly the information youâ€™re looking for without spending too much time
poring over page after page of search results. Operators are used to refine the results and to maximize the
search value. They are your tools as well as Hacker's weapons.
weapons
They are two types of Google operators:-
operators:
- Basic Operators
- Advance Operators

Google is a search engine. (Google, Bing, Yahoo, rediff, DuckDuckGo, etc.)
Google is a search engine, Basic principal of the search engine is that search engine visits the website, and each search engine has its own unique algorithm. The biggest reason for being Google's fame is its speed, before Google's era was Yahoo's era. When Yahoo used to do slow search, it used to take more time. Google did the work for reducing the time of this search. Google updated its algorithm, made some necessary changes so that the search result that it has, it can be represented to you quickly.
Google visit the website and store page url, page heading, page h1 content, page h2 content, title tag, alt tag, meta tag and some more html tags in the database.

Google visits the website and indexes the page url, page heading, page h1 content, page h2 content, title tag, alt tag, meta tag and some more html tags.

When the website is created, before the implementation of the website the website is designed , before the design the website is analyzed that how is the website. When the website is created by the developer, then there may be some pages or urls, that store sensitive information while creating the website. And at that time the website has been live. and at that time Google come to the website, And Google has indexed the pages of the website. and it may be that after the website is created, those pages have not been removed on the last review of the website.

So suppose if the website ever gets hacked, then Google can also be behind it, because the data that Google had indexed was sensitive. So we wil search same / some sensitive data here. via google hacking database:

some sensitive information :
in the comment section of any page
not proper configuration on server side or may be directory listing is enable
any backup placed on the server
any admin panel url that axist before and so more.

we wll search heare any kind of information lik of the related website via google search.

Whatever we search on Google, it is called keyword. Keywords are short tell, medium tell, and long tell.

google is search engie that indexes no of pages and some more information.

Google search :

ethical hacking course in indore - About 1,60,000 results (0.73 seconds)Â

ethical hacking -
About 3,38,00,000 results (0.63 seconds)Â

ethical -
About 3,37,00,00,000 results (0.63 seconds)Â

hacking -
About 4,32,00,00,000 results (0.57 seconds)Â

course -
About 4,59,00,00,000 results (0.68 seconds)Â

keyword is small result of search volume is more, keyword is long result of search volume is less.

when we get any application or organization name we search on google may be we get some information about the application or organization.

in google search we can use operators with database.
in the database when we searching any kind of data we can use operators with database.

by oprators we can narrow search result or wide. here we focus on narrow.

To narrow the search result we can use basic operators and Advance operators with database.

Basic Operators: - (+, -, , ~, ., *, "", OR)

+ (force inclusion of something common)
Using + forces Google to include a particular keyword. Its includes all pages where both keywords occur.
Do not put a space after the â€œ+â€ .
Example:
google +hacking

- (exclude a search term)
The minus operator does reverse. It gives you search results without the keyword placed after the
operator. Do not put a space after the â€œâ€“â€œ
google -hacking

~ (suggests â€˜similar)
The tilde symbol generally suggests â€˜similar toâ€™.
~google hacking

~ (suggests â€˜similar)
The tilde symbol generally suggests â€˜similar toâ€™.
~google hacking

.(search within a range)
double dots help you to search within a range of two numbers.
laptop $300..$500

*(missing keywords)
Asterisk
sterisk operator is handy when you are sure of more keywords are missing.
"how to hack *"

â€œ â€ (contain keyword in same form)
Surround a word or a phrase with double forces Google to search for pages that contain it exactly in the
same form.

"google hacking"

OR (compare with between keyword)
Using OR (in uppercase) with two or more keywords tells Google to search for pages that contain either
of the words.
windows OR linux

hacking +ethical About 6,46,00,000 results (0.61 seconds)

hacking -ethical About 6,36,00,00,000 results (0.56 seconds)

~hacking About 3,96,00,00,000 results (0.54 seconds)

how to hack~ About 4,05,00,00,000 results (0.33 seconds)

iphone $1000....$1500 About 85,400 results (0.37 seconds)Â

windows or linux About 4,17,00,00,000 results (0.61 seconds)Â

windows and linux About 4,96,00,00,000 results (0.64 seconds)Â

Advance Operators:-

Rules:
â€¢ No space between the operator and the search term
    - intitle:anycompanyname

â€¢ If a space exists in the search term, use " ". Or use a period.
    - intitle:"anycompany name"
    - intitle:example.com

â€¢ Searches
    o searches are NOT case sensitive

â€¢ combine most operators
    o intitle:"ethical hacking" filetype:pdf

â€¢ intitle :- Restricts your search to the titles of web pages.

intitle:hacking
About 43,70,000 results (0.73 seconds)Â

intitle:ethical+hacking
About 3,38,000 results (0.65 seconds)Â

intitle:"ethical hacking"
About 2,30,000 results (0.64 seconds)Â

intitle:"Company Name"
About 713 results (0.71 seconds)Â

â€¢ allintitle :- finds pages wherein all the words specified make up the title of the web page.

allintitle:ethical+hacking
About 2,27,000 results (0.78 seconds)Â

allintitle:"ethical hacking"
About 2,30,000 results (0.60 seconds)

â€¢ inurl:- Restricts your search to the URLs of web pages.

inurl:ethical-hacking
About 1,27,000 results (0.53 seconds)Â

inurl:ethical%20hacking
About 835 results (0.48 seconds)Â

â€¢ allinurl:- finds all the words listed in a URL

allinurl:ethical-hacking
About 1,27,000 results (0.53 seconds)Â

allinurl:ethical%20hacking
About 4 results (0.26 seconds)Â

â€¢ intext :- searches only body text (i.e., ignores link text, URLs, and titles).

intext:"ethical hacking"
About 97,30,000 results (0.81 seconds)Â

â€¢ site:- allows you to narrow your search by either a site or a top-level top domain.

site:https://example.com
About 360 results (0.17 seconds)Â

site:https://example.com password Page 6 of about 49 results (0.41 seconds)Â

site:https://example.com backup About 38 results (0.36 seconds)Â

site:.com
About 25,27,00,00,000 results (5.84 seconds)Â

site:.gov.in
About 4,27,00,000 results (0.32 seconds)Â

site:.gov.in wp-admin
About 1,16,000 results (0.43 seconds)Â

site:.gov.in inurl:wp-login.php
10 results (0.27 seconds)Â

site:.gov.pk admin
About 1,63,000 results (0.30 seconds)Â

site:example.com
About 360 results (0.21 seconds)Â

â€¢ filetype :- searches the suffixes or filename extensions. These are usually, but notnecessarily, different

filetype:pdf hacking
About 3,42,00,000 results (0.48 seconds)Â

filetype:pdf hacking site:example.com About 4 results (0.30 seconds)Â

â€¢ inanchor :- searches for text in a page's link anchors. A link anchor is the descriptivetext of a link.

inanchor: companyname
About 68 results (0.70 seconds)Â

â€¢ link: : returns a list of pages linking to the specified URL.

link:companyname
About 8,410 results (0.56 seconds)Â

â€¢ cache: : finds a copy of the page that Google indexed.

cache:www.example.com
(when google visit the website)

â€¢ info: : provides a page of links to more information about a specified URL.

info:www.example.com
About 88,500 results (0.65 seconds)

â€¢ related: : as you might expect, finds pages that are related to the specified page.

related:www.yahoo.comÂ

index.of.dcim

index.of.password

index.of.password filetype:txt

ndex.of.password filetype:sql

index.of.private

index.of.backup

index.of.backup zip

index.of.backup site:gov.in

index.of.password site:gov.in

site:gov.in username password filetype:txt

username password filetype:txt @gmail.com

username password filetype:txt @hotmail.com

username password filetype:txt .gov.in

username password filetype:txt example.com

godaddy username password filetype:txt

paytm username password filetype:txt

paypal username password filetype:txt

payu username password filetype:txt

filetype:txt Card Number Exp Date cvv

filetype:xls Student Name indore

inurl:webarch/mainframe.cgi

intitle:"multimon ups status page"

intitle:"SpeedStream Router Management Interface"

Mailid@gmail.com

987654321 pdf / txt

Hacking Printers, Power Systems and Routers
Printers

inurl:webarch/mainframe.cgi

UPS (Power Systems)

intitle:"multimon ups status page"

Hacking Routers

intitle:"SpeedStream Router Management Interface"

intitle: VNC Viewer From Java

intitle:"sipura.SPA.Configuration" -.pdf

Google Dork (Google Hacking Database)

https://www.exploit-db.com/google-hacking-database

inurl:adminpanel site:gov.*

intitle:"index of" "wp-config.php.bak"

site:*/wp-admin/install.php intitle:WordPress Installation

site:apple.com

site:apple.com -www -developer -news -apps -tv -support -authors -music -itunes etc.

site:apple.com inurl:wp-admin

site:apple.com inurl:phpmyadmin

site:apple.com inurl:phpmyadmin -books

site:example.com inurl:php

site:example.com intext:php

theHarvester -d example.com -l 500 -b google
metagoofil -d example.com -l 20 -t pdf -n 20 -o doc

Shodan

Shodan is a search engine that lets users search for various types of servers (webcams, routers, servers, etc.) connected to the internet using a variety of filters.

https://www.shodan.io/

Shodan is a search engine, basicaly we can call it device search engine, here we get information of devices and servers, it is not a content search engine, we cannot search content here, here we will get technology related information or device related information, Its working principle is simple, it goes to the server and indexes the server. what is the server, what is the name of the server, what is the version, what is the port on which the server is running, what is the ip of the server. shodan stores the information of the device.

we search heare according to our scop. (we should know what is the our scop)

search:

example.com (search the taget url / domain / whatever the scop / organization name)

Companyname

(shoda may be store the related target organization data)

You can search the information of the recently found vulnerability on Shodan, because Shodan already has information about the servers of many organizations, and we can find that which organization those servers belong to, so that we can report the new vulnerability to those organizations. (if we manualy find servers so its take more time. so we can search on shodan)(all device which is connected from internet showdan indexes those device.)

filtername:value (https://www.shodan.io/search/filters)

Filter Name	Description	Example
city	Name of the city	city:"indore"
country	2-letter Country code	country:IN
http.title	Title of the website	http.title:"Ethical Hacking"
net	Network range or IP in CIDR notation	net:8.8.0.0/16
org	Name of the organization that owns the IP space	org:Google
port	Port number for the service that is running	port:22
product	Name of the software that is powering the service	product:Samsung
screenshot.label	Label that describes the content of the image	screenshot.label:ics
state	U.S. State	state:TX

port:21 (all those Servers on which FTP is running.)

port:21 org:"GoDaddy.com, LLC" (all GoDaddy Servers on which FTP is running.)

port:8080 org:"GoDaddy.com, LLC" (all GoDaddy Servers on which apaache tomcat is running)

city:"indore" (all those Servers which is from indore)

city:"indore" org:"Rajesh Patel Net Services Private LTD" (all Rajesh Patel Net Services Private LTD Servers which is from indore)

city:"indore" port:445 (all those Servers which is from indore and services running on port 455 .)

city:"indore" port:3389 (all those Servers which is from indore and RDP running on port 3389 .)

city:"indore" port:5900 (all those Servers which is from indore and VNC running on port 5900 .)

vuln:MS17 (all eternal blue vulnerable servers)

net:8.8.8.8/24 (searching network range / whatever ip or network we get for pentest search here)

hostname:google (result shown according to google host name)

OS:"Windows XP" (all windows xp servers)
OS:"Windows 7" (all windows 7 servers)

OS:"Windows 7" port:445 (all windows 7 servers on which 445 is running.)

country:'IN' (all server from INDIA)

country:'IN' port:80

country:'IN' port:445

country:'IN' port:445 os:'windows 7'

geo:'32.8000000-117.00000000' (geographical location value by longitude and lantitude)

title:'phpmyadmin' (all phpmyadmin running servers) (search by title)

title:'apaache' (all apaache running servers)

product:'Apache httpd' (all apache httpd servers)

product:'Apache httpd' org:'apple Inc'

we can use shodan by command line using shodan api configure to follow link: https://help.shodan.io/guides/how-to-download-data-with-api

$ sudo easy_install shodan
$ sudo apt-get install python-setuptools
$ shodan
$ shodan init YOUR_API_KEY

$ shodan download --limit <number of results> <filename> <search query>

$ shodan download --limit 500 mongodb-results product:mongodb

$ shodan parse --fields ip_str,port --separator , mongodb.json.gz

$ shodan search net:129.26.0.0/22

start with Target

Scop

https://www.calculator.net/ip-subnet-calculator.html

129.176.0.0/22	129.176.0.1 - 129.176.3.254
129.176.16.0/24	129.176.16.1 - 129.176.16.254
129.176.4.0/25	129.176.4.1 - 129.176.4.126

IP t Location https://www.iplocation.net/

129.176.0.1

Mayo Foundation for Medical Education and Research

ASN Lookup https://spyse.com/tools/asn-lookup

ASN AS7973

129.176.0.0/16 this all ip have Mayo Foundation for Medical Education and Research

Our Scop is :

129.176.0.0/22	129.176.0.1 - 129.176.3.254
129.176.16.0/24	129.176.16.1 - 129.176.16.254
129.176.4.0/25	129.176.4.1 - 129.176.4.126

not all of 129.176.0.0/16

Shodan Search:

net:129.176.0.0/22

Total Results
154

Top Ports
â€¢ 44379
â€¢ 8054
â€¢ 214
â€¢ 223
â€¢ 130003
â€¢ 27622
â€¢ 50602
â€¢ 200002
â€¢ 52221
â€¢ 80811
â€¢ 84431
â€¢ 88851

Top Products
â€¢ BigIP49
â€¢ Apache httpd2
â€¢ nginx2
â€¢ Microsoft IIS httpd1
â€¢ Ncat http proxy1
â€¢ "TANDBERG/4137 (X1

Brows all the result and overview what is running there.

129.176.2.71

#dig -x 129.176.2.71
nslookup 129.176.2.71

alertus.mayo.edu

brows 129.176.2.71
brows alertus.mayo.edu

129.176.1.138

#dig -x 129.176.1.138

dev.dtapi.mayoclinic.org

brows 129.176.1.138 (not found)
brows dev.dtapi.mayoclinic.org (running website)

check by builtwith or wapalyzer what web site built with what technology use.

#dig -x dev.dtapi.mayoclinic.org (check dev.dtapi.mayoclinic.org belong to ip)

https://dev.dtapi.mayoclinic.org/swagger/ui/index

129.176.2.7

#dig +short -x 129.176.2.7
ftp.mayo.edu.

ftp 129.176.2.7
try default login password

129.176.3.58
http://129.176.3.58/ 403 - Forbidden: Access is denied.(no index page or not enable directory listing)
https://129.176.3.58/ 403 - Forbidden: Access is denied.(here in favicon icon some info that what was befor thare)

#dig -x 129.176.3.58
lws.mayo.edu.

brows lws.mayo.edu 403 - Forbidden: Access is denied.

129.176.1.87

dig +short -x 129.176.1.87
mayoclinichotline.edu.
mwredirects4.mayo.edu.
mayoemployees.org.
bioservices.mayoclinic.com.mayo.edu.

Brows mayoclinichotline.edu
Brows mwredirects4.mayo.edu
Brows mayoemployees.org
Brows bioservices.mayoclinic.com.mayo.edu

Shodan Search:

net:129.176.0.0/22 port:8080
net:129.176.0.0/22 port:8081

https://129.176.1.106:8081/ (not found)

net:129.176.0.0/22 port:445

net:129.176.0.0/22 port:21

Total Results

4

129.176.2.7
129.176.1.203
129.176.1.204
129.176.1.205

may be ftp version burnable check it

ftp 129.176.1.205 try default login password (try to run any command some tiome may be connection make but ftp say invalid)
ftp 129.176.1.204 try default login password
ftp 129.176.1.203 try default login password
ftp 129.176.2.7 try default login password

dig +short -x 129.176.2.7
ftp.mayo.edu.

dig +short -x 129.176.1.203
mftportal.mayo.edu.

dig +short -x 129.176.1.204
gf.test.mftportal.mayo.edu.

dig +short -x 129.176.1.205
gf.sandbox.mftportal.mayo.edu.

ftp gf.sandbox.mftportal.mayo.edu (try ftp login by also name)
ftp mftportal.mayo.edu
ftp gf.test.mftportal.mayo.edu
ftp gf.sandbox.mftportal.mayo.edu

brows https://ftp.mayo.edu
brows https://mftportal.mayo.edu
brows https://gf.test.mftportal.mayo.edu
brows https://gf.sandbox.mftportal.mayo.edu

if by comman id password ftp get login then ftp is vulnerable and after if we get some sensative info than this belongs to p1 vulnerability othervise its belong to p1

Shodan Search:

net:129.176.0.0/22 port:80

net:129.176.0.0/22 port:3389
net:129.176.0.0/22 port:3306
net:129.176.0.0/22 port:8000
net:129.176.0.0/22 port:8443

brows https://129.176.2.186:8443
brows https://129.176.2.187:8443 (here is big ip router, if big ip router have some vulnerability than we can exploit it)

dig +short -x 129.176.2.186
randohub-dev.mayo.edu.

dig +short -x 129.176.2.187
randohub.mayo.edu.

browshttps://randohub-dev.mayo.edu:8443
brows https://randohub.mayo.edu:8443

(if we have more ip so we can applay same approch on all ip then next approch applay on all ip check one port on all ip then check next port on all ip dont go one by one ip because it take more time check continue one port and same aproch we can apply on all ip and we can apply same approch on all ip and our focus on one protocol at the time.)

Shodan Search:

net:129.176.0.0/22 port:13000

129.176.0.42
129.176.0.26
129.176.0.43

browshttps://129.176.0.42:13000
browshttps://129.176.0.26:13000
browshttps://129.176.0.43:13000

dig +short -x 129.176.0.42
qa.mmlaccess.com.

dig +short -x 129.176.0.26
mmlaccess.com.
gfld.mmlaccess.com.

dig +short -x 129.176.0.43
test.mmlaccess.com.

Shodan Search:

net:129.176.0.0/22 port:2762

129.176.2.55
129.176.2.56

browshttps://129.176.2.55:2762 (some database protocol here)
browshttps://129.176.2.56:2762

dig +short -x 129.176.2.55
rportal.mayo.edu.

#dig +short -x 129.176.2.56
rportal2.mayo.edu.

browshttps://rportal.mayo.edu
browshttps://rportal2.mayo.edu

Shodan Search:

net:129.176.0.0/22 title:phpmyadmin

we can use shodan by command line using shodan api configure to follow link:
https://help.shodan.io/guides/how-to-download-data-with-api

$ shodan init YOUR_API_KEY
$ shodan search net:129.176.0.0/22

On git hub All the things here we have to search according to the target.

ip to location https://www.iplocation.net/

129.176.16.1

https://host.io/mayoclinic.com
(organization name is imporant if we penetrate network)
Mayo Foundation for Medical Education and Research

Github seaarch: Mayo Foundation for Medical Education and Research

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ password

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ key

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ credantial

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ secret

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ api

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ token

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ login

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ ftp

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ config

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ ssh

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ filename:wp-config

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ filename:htpasswd

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ filename:bash_history

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ filename:ftpconfig

Github seaarch: â€œMayo Foundation for Medical Education and Researchâ€ filename:webserver.xml

Github seaarch: filename:webserver.xml password

Github seaarch: filename:webserver.xml username password

Github seaarch: filename:wp-config.php

Github seaarch: â€œ.gov.inâ€ filename:wp-config.php

Github seaarch: â€œ.comâ€ filename:wp-config.php

Github Recon

GitHub

GitHub is a Git repository hosting service, but it adds many of its own features. While Git is a command line tool, GitHub provides a Web-based graphical interface. It also provides access control and several collaboration features, such as a wikis and basic task management tools for every project.

Through Geet Hub, we can publish the source code of our code, application, project or scripts, and share it with the developer. Through Geet Hub, we can manage the project, if no one person can make a big project, then more than one person works for this, through this platform more than one person can do teamwork on a project. and can easily complete the project. Project is easily managed through this platform.

Here we can get some piece of code, maybe inside that code we can get some kind of authentication like id password, maybe ssh key, maybe some kind of token, maybe That we get the source code of the application and then we can analyze that code and get any vulnerability.

Find sitemap.html, sitemap.xml, robots.txt

> sitemap.html - user index
> sitemap.xml - Search engin index
> robots.txt - Disallow for any user agent and google / search engine

(example:- https://www.example.com/sitemap.xml)

Create sitemap Online

https://www.xml-sitemaps.com/
https://www.convertcsv.com/url-extractor.htm

seo spiser

https://www.screamingfrog.co.uk/seo-spider/

Locally Mirroring the website - Read Source Code

wget

wget -m https://www.example.com

HTTrack
httrack https://www.example.com

Waybackmachine

https://archive.org
https://archive.ph/