Practical No 1

DNS Enumeration:

DNS name server and mail server enumeration with dnsenum tool

Syntax: dnsenum <domain name>

Ex: dnsenum example.com

DNS sub-domain enumeration with dnsdict6

Syntax: atk6-dnsdict6 -d46 <domain name>

Ex: atk6-dnsdict6 –d46 example.com

DNS VOIP phone enumeration with dnsrecon

Syntax: dnsrecon -t srv -d <domain name>

Ex: dnsrecon -t srv -d example.com

Practical No 2:

Web site technical information gathering using whatweb tool

This tool will give you information about the target ip, web server fingerprint, server location, back-end app engine along with version number, and any other technical information like google analytics id etc.

Syntax: whatweb -v <domain name>

Ex: whatweb -v example.com

Practical No 3:

Web site technical information gathering using OWASP mantra browser

Please go to <u>http://www.getmantra.com</u> and download the suitable version of OWASP mantra for your pc and install it as soon as it completes.

OWASP mantra is a hacker friendly browser which includes all hacking plugins inbuilt in the browser itself so no need to install them separately.

In this browser whatever website you are trying to open OWASP mantra will automatically get the website information for you.

Practical No 4:

Google Dorks:

intitle

Specifying intitle, will tell google to show only those pages that have the term in their html title. For example intitle:"login page" will show those pages which have the term "login page" in the title text.

allintitle

Similar to intitle, but looks for all the specified terms in the title.

inurl

Searches for the specified term in the url. For example inurl:"login.php".

allinurl

Same as inurl, but searches for all terms in the url.

filetype

Searches for specific file types. filetype:pdf will looks for pdf files in websites. Similarly filetype:txt looks for files with extension .txt

ext

Similar to filetype. ext:pdf finds pdf extension files.

intext

Searches the content of the page. Somewhat like a plain google search. For example intext:"index of /".

allintext

Similar to intext, but searches for all terms to be present in the text.

site

Limits the search to a specific site only. site:nullbyte.com

So you can mix them up to find out cameras like this

Inurl:/view/index.shtml

One of the link was opened below and you can see an airport view with planes in it.



We will get even more, but I thought for example one is enough.

If you want more camera google dorks you can follow the below link

http://members.upc.nl/a.horlings/doc-google.html

If you want to find out google dorks other than cameras you can follow this link <u>http://www.exploit-db.com</u>

There you can find out google dorks for different categories like files containing usernames, files containing passwords like that.

Practical No: 5

You can visit the website searchdns.netcraft.com for gathering information like the hosting history, and site technologies, OS they run on their webservers and the webserver versions etc.

Step 1: open searchdns.netcraft.com website.

Arctart Services Nature Name And-Rhining Toolar Phishing Steader Prishing Steader Countermeasures Audded by Netrona Open Redired Delection Web Application Security Web Application Security Wold Redired Delection Web Application Security Web Application Security Multion Busiest Websites Noting Provider Switching Analysis Hosting Provider Switching Noting Provider Switching Noting Provider Switching Noting Provider Switching Noting Provider Switching Nature Statement Statement Statement Statement Moting Reselier Survey Statement	HETCRAFT			
Netrat News ship & Security Anti-Phishing Sile Feed Hosting Phishing Alerts Frau Detection Phishing Sile Feed Hosting Phishing Alerts Frau Detection Open Redirect Detection Web Application Security Coper Redirect Detection Web Application Security Conser Million Busiest Webates Hosting Provider Switching Hosting Reseller Survey SSL Survey			Apventise	MENT (
Netrait News Bing A Security Bin March 2015 Anti-Phishing Tollobr Bin March 2016 Phishing Site Feed iste containsscorth iss Hosting Phishing Alerts iste containsscorth iss Fraud Delection Iste containsscorth iss Phishing Site Feed iste containsscorth iss Open Redirect Delection COPYRIGHT @ NETCRAFT LTD 2016. ALL RIGHTS RESERVED. Audited by Netoral COPYRIGHT @ NETCRAFT LTD 2016. ALL RIGHTS RESERVED. Audited by Netoral COPYRIGHT @ NETCRAFT LTD 2016. ALL RIGHTS RESERVED. Web Application Security Feeling Testing State	tcraft Services	Search Web by Domain		
shing Security Explore 1,516,940 web sites visited by users of the Netrat Toolbar: Bit March 2016 Anti-Phishing Toolbar search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search: search:	Netcraft News			
Anti-Finandig looded Phishing Sife Seed Hosting Phishing Sife Seed Search: search tips Fraud Detection Phishing Sife Seed Countemeasures Audited by Neticraft Open Redirect Detection Web Application Security Testing Web Application Security Course Million Busiest Websites Hosting Provider Switching Hosting Reseller Survey SSL Survey	shing & Security	Explore 1,516,940 web sites visited by users of the Netcraft Toolbar 8th March 2016		
Hosting Phishing Alerts Fraud Detection Prishing Site Ountermeasures Audied by Netraft Oper Redirect Detection Web Application Security Testing Web Application Security Course Intermeasures Million Busiest Websites Hosting Provider Server Count Count Reseller Survey St. Survey	Phishing Site Feed	Search: search tips		
Fraud Delection example: site contains .netcoft.com Phishing Site COPYRIGHT © NETCRAFT LTD 2016. ALL RIGHTS RESERVED. Audited by Netcraft Open Redirect Detection Web Application Security Vesting Provider Switching Million Busiest Websites Hosting Provider Switching Hosting Reselier Survey SSL Survey	Hosting Phishing Alerts	site contains 🔻 Iookupl		
Phishing Site Countermeasures Audited by Netcraft Open Redirect Detection Web Application Security Testing Web Application Security Roting Forwider Switching Analysis Hosting Reseiler Survey SSL Survey SSL Survey	Fraud Detection	example: site contains .netcraft.com		
Countemessures CopyRIGHT © NETCRAFT LTD 2016. ALL RIGHTS RESERVED. Web Application Security Testing Web Application Security Course Tert Data Mining Million Busiest Websites Hosting Provider Switching Analysis Hosting Reseller Survey SSL Survey Tert Exploration	Phishing Site			
Notion of Nettern Veb Application Security Testing Web Application Security Course Tere Cata Mining Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey SSL Survey Tere Exploration	Countermeasures	COPYRIGHT © NETCRAFT LTD 2016. ALL RIGHTS RESERVED.		
Web Application Security Testing Web Application Security Course Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey S&L Survey	Open Redirect Detection			
Testing Web Application Security Course Teret Data Mining Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey SSL Survey Teret Exploration	Web Application Security			
Web Application Security Course ernet Data Mining Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey SSL Survey ernet Exploration	Testing			
ernet Data Mining Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey servet Exploration	Web Application Security Course			
Million Busiest Websites Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey struct Exploration	ernet Data Mining			
Hosting Provider Switching Analysis Hosting Provider Server Count Hosting Reseller Survey SSL Survey	Million Busiest Websites			
Hosting Provider Server Count Hosting Reseller Survey SSL Survey	Hosting Provider Switching			
Count Hosting Reseller Survey SSL Survey	Hosting Provider Server			
Hosting Reseller Survey SSL Survey ernet Exploration	Count			
SSL Survey ernet Exploration	Hosting Reseller Survey			
ernet Exploration	SSL Survey			
	ernet Exploration			

Step 2: enter your domain in search bar and hit lookup button. So you will get result like shown in the below image.

C B searchdns.netc	raft.com/?restriction=site+co	ntains&host=wipro.com&loc	kup=wait&positio	n=limited		5
etcraft Services	Search Web by D	omain				Apventeeseer
ishing & Security	Explore 1,516,940 web sites visite	ed by users of the Netcraft Toolbar			8th March 2016	
Phishing Site Feed		Search:		search tips		
Hosting Phishing Alerts		site contains	wipro.com	lookup!		
Fraud Detection		exar	nple: site contains .netcraft	.com		
Phishing Site						
Countermeasures	D	9111-04031				
Open Redirect Detection	Results for wipro.	com				
Web Application Security Testing	Found 17 sites					
Web Application Security	Site	Site Report	First seen	Netblock	05	
Course	1. mywipro.wipro.com	6	january 2010	wipro technologies	unknown	
ernet Data Mining	2. careers.wipro.com	6	march 2002	microsoft corp	windows server 2008	
Million Busiest Websites	3. www.wipro.com	6	december 1995	wipro technologies	unknown	
Hosting Provider Switching	4. gateway.wipro.com	6	january 2012	wipro technologies	f5 big-ip	
Hosting Provider Server	5. helpline.wipro.com	1		wipro technologies	unknown	
Count	6. knowledge.wipro.com	1	december 2014	wipro technologies	windows server 2008	
Hosting Reseller Survey	7. kmsites.wipro.com	1	october 2013	wipro technologies	windows server 2008	
SSL Survey	8. wipro.com	1	march 2000	wipro technologies	unknown	
ernet Exploration	9, webmail.wipro.com	1		wipro technologies	unknown	
Whats that site running?	10. north-west.wipro.com	1	march 2011	ibis inc.	unknown	
SearchDNS	11. newitms.wipro.com	1		microsoft	unknown	
Sites on the MOVE	12. itms.wipro.com	1		wipro technologies	unknown	
formance	13. serviceconnect.wipro.com	1		wipro technologies	unknown	
Hosting Prospects	14. cf1.wipro.com	6	febuary 2011	wipro net ltd,	windows server 2003	

You can get instant results like OS, netblock and firstseen details of the respective domain names.

If youwant more details apart from them click on the site report page icon to get them. Shown in the below image.



Practical No: 6

IP tracking using tracking mail

We can track the victim ip address by sending him an email tracking script to his email for this purpose you can use lot of services, one of them is readnotify.

Follow the below given steps to track an ip address of the victim.

Step 1: open readnotify.com and create an account in that website.

For free account you can send up to 25 ip tracking emails.

Step 2: after logging inside of the website just go towards bottom right corner. There you can find out "member utilities" hover your mouse over that object you can observe a list will appear, select "email quick send" option,

Step 3: on the email quicksend option compose email according to requirement and make sure you add your target email id in the "To" text field along with you target email id append ".readnotify.com" extra like this

target@gmail.com to target@gmail.com.readnotify.com

and eventually click on the send button.

Step 4: now again hover your mouse over member utilities and this time select "personal tracking page"

There you can see the list of emails you send to all the victims till now, If he opens your email you can see opened date and time. Click on the date and time to see what ip address the victim is using on that time.

Practical No 7: Using Robtex.com website to get the target website network structure.

Step 1: Go to robtex.com

C Robtex X	≛ - ¤ ×
← → X 🔓 Robtex LTD [CY] https://www.robtex.com	යි <mark>🗖</mark> 🔳
Robtex	
Over 20.000 teams use DigitalOcean FIND out MORE	
hostname/ipnumber summany forward reverse similar scorecard shared graph	
domain name, ip number, as number, route	
G+I 11k	
Welcome to the new robtex! This is a beta release, and it does not yet have all information available at our old site, but it will come together with new data that is not available of	even there.
We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet	
Waiting for www.robtex.com 'e guess that is not a secret anymore, and no we didn't know before either). Are you a normal IT	guy doing data
	へ 🗐 🦟 ଏ× 📮 7:36 PM 3/12/2016

Step 2: Enter your target domain name or IP address into the input box

C Robtex LTD [CY] https://www.rob	t ex.com /?q=juggyboy.com		☆
	Over 20,000 teams use DigitalOcean		
juggyboy.com summary forward	reverse similar scorecard	shared graph	
Share 0 G+1 0 get showing 8 result(s)	1		
juggyboy.com ?dns=juggyboy.com host name juggyboy.com			
iuggrber co			

Select the website from the results

Step 3: scroll down to see the network diagram.

/ 🕼 juggyboy.com 🗙	*	- 0	>	<
← → C C Robtex LTD [CY] https://www.robtex.com/?dns=juggyboy.com		Q	Π	≡
ab-in-xta.lel00.net ePTR PTR 2404:6600:4003:c01::1a MX1s aspex3.googtemail.com A AA				
de=in=xtb.1e100.net PTR PTR 2a00:1450:400b:c02::1b MX* alt2.aspxc.1.google.com PA A4				
MX* MX* A <td></td> <td></td> <td></td> <td></td>				
juggyby, com MX MX A NSV NSV MSV A agms2.googlemail.com A DTO DTO DTO DTO DOD::10				
wm-in-f27.1e100.net An 64.233.166.27 64.233.166.0/24 Google bgp A bgp A bgp A de-in-f27.1e100.net ePTR 74.125.24.27 *bgp bgp* 74.125.24.0/24 Google bgp A bgp A bgp A				
Av 74.125.130.26 bbgp bgp* 74.125.130.0/24 Google bbgp wb-in-f26.1e100.net ePTR PTR PTR bbgp bgp* 74.125.130.0/24 Google bbgp wb-in-f26.1e100.net ePTR PTR I73.194.73.26 bbgp bgp* 173.194.73.0/24 Google bbgp				
Art Distribution Distribution <thdistribution< th=""> Distribution</thdistribution<>				
	^ ₩⊒ <i>(</i> (¢× 📮	7:37 PN 3/12/20	И 16

Practical No 8: Using Who.is website to get domain owners information

Step 1: Go to who.is		
C WHOIS Search, Domain N ×		≛ – ¤ ×
← → X 🗋 who.is		යි 🗖 \Xi
	Premium Domains Transfer Features Log In	Sign Up 🗎
	WHOIS Search, Domain Name, Website, and IP Tools	
	Search Domain name or IP address Q	
	Your IP address is 49 204 16.70	
	poking to get a website? 🚨 Web Hosting 🔅 Website Builder 🖀 SSL Certificates	
	Get started on your website today	
Waiting for cache_	Choose the option below that best describes your website project. We'll recommend a package of products and services, and then you can fine tune everything.	
📲 🔎 📼 🔚 🌖 😂 🍋		^ 100

Step 2: Enter your target domain name or IP address into the input box



Step 3: Get the domain registration information (probably the owner information)

