

# LAB MANUAL ON VULNERABILITY ASSESSMENT & PENETRATION TESTING



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY GOVERNMENT OF INDIA Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

**PREPARED BY:** 

Prof. Maitreyee Dutta and Mr. Vipul Mandhar (Project Assistant)

#### Table of Contents

What is VAPT?
Vulnerability Assessment4
Penetration Testing4
What is the difference between a Pen Tester and a Hacker?
Difference between Penetration Testing and Vulnerability Assessment?6
Vulnerability Assessment:
Penetration Testing:6
Scope of Penetration Testing6
Why Bother?
Active pen-testing teaches you things that security planning will not .8
Raises security awareness8
Types of Testing
Penetration Testing at Ames
Network Vulnerability Testing10
ABOUT ASSUMPTIONS:10
Rules of Engagement:10
Web Vulnerability Testing10
Wireless War Driving / Walking11
Phone Network Tests12
Social Engineering / Phishing Tests12
Walk-throughs and Dumpster Diving13
Goal: See what kind of sensitive information your employees are leaving in:
Physical security auditing13
1

Common things to look for:
Physical Sec: Safety Considerations14
High Level Outputs
Training and awareness14
Trends for ARC since inception of program:14
Why VAPT?
Cybersecurity Myths for SMEs16
Audit vs Penetration testing?17
Why do SMEs need VAPT?
Basic security measures are not enough
Security budget
Reputation18
SMEs also lose out on potential/existing business
Company: Fortnite / Online Gaming19
Instagram / Social Media19
Methodologies19
Used Methodology
The Problem
IDEA20
How to Start ?
01. Planning21
02. Foot Printing21
03. Exploiting
04. Reporting & Compare
Future Work
Practical Implementation
2

HTTrack	23
How to Download HTTrack	23

# What is VAPT?

#### **V-Vulnerability**

#### **A-Assessment**

#### **P-Penetration**

#### **T-Testing**

# Vulnerability Assessment

A process to evaluate and review key systems, networks and applications. To identify vulnerabilities and configuration issues that may put the organization at risk of being breached or exploited Effective in identifying vulnerabilities, but it cannot differentiate between exploitable vs nonexploitable vulnerabilities

# **Penetration Testing**

Goal-driven test focused on identifying all possible routes of entry an attacker could use to gain unauthorized entry into the target. Identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Proof of concept strategy to investigate, exploit and validate the extent of the identified vulnerability.

# What is the difference between a Pen Tester and a Hacker?

- Pen Testers have prior approval from Senior Management
- Hackers have prior approval from themselves.
- Pen Tester's social engineering attacks are there to raise awareness
- Hackers social engineering attacks are there to trick the DMV into divulging sensitive information about the where abouts of their estranged ex-spouse.
- Pen Tester's war driving = geeks driving cars with really long antennas, license plate reading "r00t3d" while dying their hair green looking to discover the hidden, unapproved networks your users thought it would be OK to install for you.
- Hackers wireless war driving doesn't happen so often because 14 year olds typically don't have their license yet.

# Difference between Penetration Testing and Vulnerability Assessment?

## Vulnerability Assessment:

- » Typically is general in scope and includes a large assessment.
- » Predictable.
- » Unreliable at times and high rate of false positives.
- » Vulnerability assessment invites debate among System Admins.
- » Produces a report with mitigation guidelines and action items.

## **Penetration Testing:**

- » Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
- » Unpredictable by the recipient. (Don't know the "how?" and "when?")
- » Highly accurate and reliable. (I've got root!)
- » Penetration Testing = Proof of Concept against vulnerabilities.
- » Produces a binary result: Either the team owned you, or they didn't.

#### Scope of Penetration Testing

Targeted Recon.

» Targeted exploitation of vulnerable software.

Social Engineering

» Hi Help Desk...I'm Mr. Jones...Can you tell me what my password is?

Physical facilities audit

» Hmm, I forgot my badge... but there's 200 yards of fence missing on the east side of the center

Wireless War Driving

» Detection of rogue or weakly encrypted AP's.

Dumpster Diving

» How much fun can I have in the dumpster...whoops...I've found someone's Tax forms with SSN.

# Why Bother?

Active pen-testing teaches you things that security planning will not.

- » What are the vulnerability scanners missing?
- » Are your users and system administrators actually following their own policies?
- » host that claims one thing in security plan but it totally different in reality
- » Audit Physical Security
- » Just what is in that building no one ever goes in?
- » The strongest network based protections are useless if there is a accessible unlocked terminal, unlocked tape vault, etc.

## Raises security awareness

- I better not leave my terminal unlocked because I know that those security guys are lurking around somewhere.
- Helps identify weakness that may be leveraged by insider threat or accidental exposure.
- Provides Senior Management a realistic view of their security posture
- Great tool to advocate for more funding to mitigate flaws discovered
- If I can break into it, so could someone else!

# **Types of Testing**



# **Penetration Testing at Ames**

- Network Vulnerability Testing
- Web Vulnerability Testing
- Wireless War Driving / Walking
- Phone Network Testing
- Social Engineering Testing
- Walk-throughs and Dumpster Diving
- Physical Security Auditing

# Network Vulnerability Testing

#### **ABOUT ASSUMPTIONS:**

- » We don't want to impact operations, so no DOS, no offensive disabling of IDS/IPS/Firewalls/etc.
- » Above assumptions impact tests, so other assumptions made. Consider though, that if you find a vuln that'd allow you to bypass IDS/IPS, that such findings cannot be used as mitigations.

#### **Rules of Engagement:**

- » Consistent with RoE document, we don't perform tests if we think they'll damage/interrupt important work.
- » Example: "Damaging" tests turned off in Nessus; SQL injection of production/mission systems; etc
- » Notify sysadmins/staff for critical and mission systems of pentest window, so they can be on hand in case of crashes, etc.
   (Note: Decreases effectiveness but is a necessary trade-off)

# Web Vulnerability Testing

During network testing, check out some of the websites your developers have put together. If possible (in scope), get permission to test sites that contractors run on behalf of NASA.

Remember, many systems now considered 'critical' are web systems throughout. An agency can be 'owned' without touching a router or system, if you nail IFMP (for example) Seen on one contractor system (the login page):

<!-- 0) SQL2K=true

CONN=Provider=SQLOLEDB;server=XXX;database=YYY;uid=ZZZ; pwd=ZZZ;SQL=undefined --->

- Fuzzers, webapp tests, OWASP. Other testing frameworks are useful here
- Consider metasploit ;)

# Wireless War Driving / Walking

- Is your campus wireless accessible from outside the campus? Have you checked? Can it be cracked?
- Drive the campus w/ Laptops equipped with 802.11, antennas if possible.
- Record any wireless network NOT authorized by the center.
- Shut down if possible!
- Bluetooth? Do the same! See what wireless shares are being broadcast (short-range) from inside locked buildings to the outsides of the building, lab, etc.
- Look for "hpsetup", "Free Public Wifi" (a worm), "linksys" and others.
- In the future, "MiFi" mobile hotspots in employees' possession are going to become numerous accidental wifi connection points.

## Phone Network Tests

- Phones? Yep, we still use 'em.
- War-dialing: Using a modem to call every number in your block looking for modems/backdoors
  - » Best done at night, or employees may get upset
- Don't forget VOIP services, Skype IDs, etc
- Use CallerID spoofing(Check with legal office) and redirection services (google voice, etc) to try to fool helpdesk staff into revealing information/passwords/etc – or to impersonate helpdesk for others

# Social Engineering / Phishing Tests

- Your users are being socially engineered and phished every day!
- They are falling for it, pretty regularly.
- Send your users a phishing email w/ Remote IP that you monitor
- Check which users download the file
- Go further! Send them a script to run; the script pings a webserver whose logs you monitor.
- Again, see who executes the file.
- Place this file on a USB thumb drive named 'Financials', drop the drive in the cafeteria
- Start a Facebook group... find people on LinkedIn... etc.

Remedial training needed for employees who respond to phsihing!

# Walk-throughs and Dumpster Diving

#### **Goal: See what kind of sensitive information your employees are leaving in:**

- » recycling/trash
- » Printer and copy rooms
- » Unlocked file cabinets
- » Unattended "archival" areas
- » Check for unlocked terminals. Check for unlocked but unattended offices w/ sensitive information in them
- Look for macguyvered IT setups in labs, offices, etc
- Use a cell phone w/ GPS tags in camera (iphone style), or GPS camera to take photos of findings. Will help with mapping problem areas, providing feedback to users.

## Physical security auditing

• Test the efficacy of your physical security controls. These are the controls we take for granted!

#### **Common things to look for:**

- » Double doors unpinned (pull n' open)
- » Door locks w/ no front plate
- » Poorly installed door locks
- » Digital door locks with default passcodes, or malfunctioning latch
- » Removable floors which extend beyond gateway doors

- » Ceilings which don't run "all the way"
- » Are your badge reader door locks fail-safe... or fail-open?
- » Circuit breakers outside sensitive areas?

# Physical Sec: Safety Considerations

- Safety precautions for pen-test team:
- Buddy system (minimum of 2 testers)
- Have a management "Bosley" for people to contact, and to run confirmation w/ police
- Have cell phone or radio contact with team members at all times
- Pre-train for safety:

# **High Level Outputs**

## Training and awareness

- » Birds of a Feather
- » Division and Directorate training
- » Management awareness
- » Reports sent to Senior Management and anyone with a need to know.
- » Security Posture reports. What is the centers risk posture?

# Trends for ARC since inception of program:

- » Significant decrease in unlocked terminals
- » Increase in reports of Spam & Phishing to Security Office.

- » Significant decrease in the amount of Sensitive information being discovered during tests.
- » More requests for All-Hands training by the Security Office.
- » Significant increase in overall Security Awareness

# <section-header>

# Cybersecurity Myths for SMEs

#### I have a firewall, so I'm safe from attacks.

- Hackers understand strategies adopted by a firewall quite well. Disrupting codes and exploiting basic ITboversights to gain access to your system is easy.
- While most cyber security threats are avoidable, your organizations can not rely solely on firewalls for protection.

#### I use HTTPS, so my site is secure

- HTTPs safeguards the transmission of information from source to destination. This is web security at a minimal.
- It does not block attacks like DDoS, brute force, injections, etc.
- There is also the issue of organizations using fake SSL certificates, resulting in their organization being compromised

#### SMEs are safe because they are not worthwhile targets

- SMEs are considered to be low hanging fruits for hackers because so many do not take security seriously.
- One of the most popular attacks that hackers use against SMEs is ransomware.

## Audit vs Penetration testing?

Audit	Penetration testing
Check set of standards	Find vulnerabilities
-	Foot printing
-	Exploiting
Create report by standards	Generate report

# Why do SMEs need VAPT?

#### Basic security measures are not enough.

• Firewalls or anti-virus solutions are not sufficient to protect against attacks.

## Security budget

- Unlike MNCs, SMEs do not have the budget to implement everything.
- There is limited or no resource for security expertise.
- What VAPT adds value to is to streamline what is needed for the organization.

## Reputation

- Potential clients or business partners will feel insecure on collaboration.
- Contributing factors can be issues like safeguard of important data.

## SMEs also lose out on potential/existing business.

 Compared to SMEs, larger organizations have a much greater potential to survive an attack due to the help of current investors and existing large clients. (E.g. Sony (04/2011) survived through the attack.)

Phishing attempts and ransomware were the most common methods used.

https://www.insurancebusinessmag.com/asia/news/breakingnews/smes-hit-by-40-of-cyberattacks-in-singapore-103736.<u>aspx</u>

#### **Company: Fortnite / Online Gaming**

In January 2019, it was announced that all 200 Million user accounts on Fortnite had been

compromised through a company-wide data breach.

https://research.checkpoint.com/2019/hacking-fortnite/

#### Instagram / Social Media

On May 20th, 2019, news broke that over 49 million Instagram influencers, celebrities, and companies had large amounts of their personal data compromised.

The data compromised included personal telephone numbers, emails, and location data.

https://techcrunch.com/2019/05/20/instagram-influencer-celebrity-accounts-scraped/

## Methodologies

- 1. Planning, Discovery, Exploiting, Reporting\*
- 2. Preparation, Anonymity, Foot Printing, Analysis, Exploiting, Reporting, Advisory\*\*
- 3. Preparation, Reconnaissance, Analysis of Information / Risks, Active Intrusion Attempts, Final Analysis / Clean-Up\*\*\*
- 4. Planning, Discovery, Attack, Reporting\*\*\*\*



Site for Penetration testing

www.penteston.com

# How to Start ?

# 01. Planning

- Test name
- Scope of Work
- Contract or NDA
- Conduct (Whitebox, Greybox, Blackbox)
- Type (Internal, External, Application-layer, Network-layer)
- Team detail

# 02. Foot Printing



• Alert Level - Low, Medium or High level of alert



# 04. Reporting & Compare



#### **Future Work**



# **Practical Implementation**

# HTTrack

HTTrack is a <u>free</u> (<u>GPL</u>, libre/free software) and easy-to-use offline browser utility.

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

Link to Download Tool for windows.

https://www.httrack.com/

# **How to Download HTTrack**

Step 1: Search for Httrack download in google.



#### Step 2: Screendump of official website of Httrack.



#### Step 3: Platform and Versions details of HTtracks.

Apps 😭 Gmail	🔹 YouTube 🧏 Maps 🔤 Wienis Lookup & IP 🍈 Network Tools by Y 👘 BuiltWith Tec	hnolo 🛐 Jeffrey Friedl's Imag — Have	e I Been Pwned: RS D	VWA - Damn Vuln
	Download HTTrack Website Copier 3.49-2			
	Platform	Choose file to download	Version	
	Windows (from Windows 2000 to Windows 10 and above) installer version WinHTTrack (also included: command line version)	httrack-3.49.2.exe [alternate site]	3.49-2 4 MiB (4195032 B) (01/Apr/2017)	
	We recommend: Windows (from Windows Vista to Windows 10 and above) 64-bit installer version WinHTTrack (also included: command line version)	httrack_x64-3.49.2.exe [alternate site]	3.49-2 4.3 MiB (4513192 B) (01/Apr/2017)	
	Windows (from Windows 2000 to Windows 10 and above) <u>without</u> installer (eg: USB key) WinHTTrack (also included: command line version)	httrack-noinst-3.49.2.zip [alternate site]	3.49-2 4.42 MiB (4635765 B) (01/Apr/2017)	
	Windows (from Windows Vista to Windows 10 and above) 64-bit <u>without</u> installer (eg: USB key) WinHTTrack (also included: command line version)	httrack_x64-noinst-3.49.2.zip [alternate site]	3.49-2 4.83 MiB (5064090 B) (01/Apr/2017)	
	Linux/OSX/BSD/Unix sources version WebHTTrack (also included: httrack, command line version)	httrack-3.49.2.tar.gz [alternate site]	3.49-2 1.75 MiB (1835077 B)	

Step 4: Choose the file to download according to system configurations.

← → C	httrack.com/page/2/en/index.html		* 💿 🛊 🥘
🏥 Apps 🛛 🖌 Gmai	🔊 YouTube 🔀 Maps 🛛 Whois Lookup & IP 💿 Network Tools by Y 🔚 BuiltWith Tee	:hnolo 🛐 Jeffrey Friedl's Imag Have	I Been Pwned: RS DVWA - Damn Vuln
	Download HTTrack Website Copier 3.49-2		
	Platform	Choose file to download	Version
	Windows (from Windows 2000 to Windows 10 and above) installer version WinHTTrack (also included: command line version)	httrack-3.49.2.exe [alternate site]	3.49-2 4 MiB (4195032 B) (01/Apr/2017)
	We recommend: Windows (from Windows Vista to Windows 10 and above) 64-bit installer version WinHTTrack (also included: command line version)	<u>httrack_x64-3.49.2.exe</u> [alternate site]	3.49-2 4.3 MiB (4513192 B) (01/Apr/2017)
	Windows (from Windows 2000 to Windows 10 and above) <u>without</u> installer (eg: USB key) WinHTTrack (also included: command line version)	httrack-noinst-3.49.2.zip [alternate site]	3.49-2 4.42 MiB (4635765 B) (01/Apr/2017)
	Windows (from Windows Vista to Windows 10 and above) 64-bit <u>without</u> installer (eg: USB key) WinHTTrack (also included: command line version)	<u>httrack_x64-noinst-3.49.2.zip</u> [alternate site]	3.49-2 4.83 MiB (5064090 B) (01/Apr/2017)

Step 5: After download file with name Httrack appears on download folder of the system.



25

#### Step 6: Click on NEXT to Install the software.



#### Step 7: Accept the agreement and click on NEXT.

Setup - WinHTTrack Website Copier		_		×
License Agreement Please read the following important information be	fore continuing	g.	Ģ	Ð
Please read the following License Agreement. You a agreement before continuing with the installation.	nust accept th	e terms of thi	is	
HTTrack Website Copier License Agreement:			~	
HTTrack Website Copier, Offline Browser for Windo Copyright (C) Xavier Roche and other contributors	ows and Unix			
This program is free software; you can redistribute modify it under the terms of the GNU General Publ as published by the Free Software Foundation; eith of the License, or any later version.	it and/or ic License er version 3		~	
I accept the agreement				
I do not accept the agreement				
<	Back	Next >	Can	cel

## Step 8: Choose the path to INSTALL the file.

Setup - WinHTTrack Website Copier	_		×
Select Destination Location Where should WinHTTrack Website Copier be installed?			Ð
Setup will install WinHTTrack Website Copier into the fe	ollowing fo	der.	
To continue, click Next. If you would like to select a different f	older, click	Browse.	
C:\Program Files\WinHTTrack		Browse.	
At least 13.9 MB of free disk space is required.			
· · ·			
< Back	Next >		Cancel

## Step 9: Click on NEXT to continue.

Setup - WinHTTrack Website Copier -	-	×
Select Start Menu Folder Where should Setup place the program's shortcuts?		ð
Setup will create the program's shortcuts in the following Start Me	nu folder.	
To continue, click Next. If you would like to select a different folder, click	Browse.	
WinHTTrack	Browse	•
Don't create a Start Menu folder		
< Back Next >	(	Cancel

#### Step 10: Select additional Task and click on NEXT.

Setup - WinHTTrack Website Copier				>
Select Additional Tasks Which additional tasks should be performed?	?		Q	J.
Select the additional tasks you would like Set Website Copier, then click Next.	tup to perform v	/hile installing W	inHTTrack	¢
Setup:				
Register WinHTTrack file types and prog	ram setup			
Additional icons:				
✓ Create a desktop icon				
Create a quick launch icon				
	< Back	Next >	Can	ncel

#### Step 11: Click on INSTALL.



#### Step 12: Click on FINISH to complete the Setup.



#### Step 13: Run the file and click on Next.

WinHTTrack Website Copier - [New	Project 1]
File Preferences Mirror Log W	indow Help
Local Disk <c:></c:>	Welcome to WinHTTrack Website Copier! Please click on the NEXT button to - start a new project - or resume a partial download
	< Back [Next > Exit Help
	29

## Step 14: Write the Project name and category.

	Project name: Project category:	↓ ▼
PerfLogs       Program Files       Program Files (x86)       Users       Public       Vipul	Type a new project nam or select existing project	e. to update/resume
anaconua android a	Base path:	C:\Users\Vipul\Desktop

## Step 15: Select the Action "Download web site" and click on NEXT.

WinHTTrack Website Copier - [Clone.v	vhtt]	
File Preferences Mirror Log Win	dow Help	
Enter Local Disk <c:></c:>		
	- Mirroring Mode -	
HoneyBOT	Enter address(es) in URL box	
My Web Sites		
PentestBox	Action:	Download web site(s)
PerfLogs		
Program Files (x86)	Web Addresses: (URL)	Add URL
Users		
Public		<u>^</u>
E. Z Vipul		
🕂anaconda		× .
.android		/
.conda	IIBL list ( tyt):	
idlerc	OTTE list (.txt).	
ipynb_checkpoi	Preferences and mirror options:	Set options
		,
3D Objects		
The late Contacts		< <u>Back N</u> ext > Cancel Help
Desktop		

30

Step 16: Open the website whose clone we want to create.

$\leftarrow \rightarrow$	C	haveibeenp	wned.com						Q	*	٢	*
Apps	🖂 Gn	nail 🚺 YouTub	e 🔀 Maps	W Whois Lookup & IP	Network Tools by Y	BuiltWith Technolo	Jeffrey Friedl's Imag	Have I Been Pwned:		DVWA	- Damn	Vuln
			0	) Hon	ne Notify me Domain searc	h Who's been pwned	Passwords API About	Donate β 🦻				
				Check if	have i b	een p\	wned?)					
			e	email address			р	wned?				
				General	te secure, unique password Why	ds for every account 1Password?	Learn more at 1Password.com					
				475 pwned websites	10,190,979,692 pwned accounts	113,739 <sub>pastes</sub>	194,794 paste acco	<b>.,870</b> <sup>unts</sup>				

Step 17: Paste the URL of the website to clone and click on NEXT.

WinHTTrack Website Copier - [Clone.whtt]	Help	
Local Disk <c:></c:>	- Mirming Mode -	
	Enter address(es) in URL box	
My Web Sites     PentestBox     PerfLogs	Action:	Download web site(s)
Program Files     Program Files (x86)	Web Addresses: (URL)	Add URL
⊡	https://haveibeenpwned.com/	
anaconda android a.conda	<	>
.idlerc ⊕ipynb_checkpoi	URL list (.txt): Preferences and mirror options:	
.ipython .jupyter .jupyter		Set options
JD Objects     Contacts		< <u>B</u> ack <u>N</u> ext > Cancel Help

Step 18: Click on I	FINISH.
E Local Disk <c:></c:>	
HoneyBOT     HoneyBOT     HoneyBOT     HoneyBOT     HoneyBOT     PerfLogs     Program Files     P	<ul> <li>Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.</li> <li>Remote connect Connect to this provider</li> <li>Disconnect when finished</li> <li>Shutdown PC when finished</li> </ul>
	On hold     Transfer scheduled for: (hh/mm/ss)     Save settings only, do not launch download now.
Journal SD Objects      Journal Contacts      Journal Desktop	< <u>B</u> ack Finish Cancel Help

Step 19: Cloning and transferring data will take some time after that click on NEXT.

Site mirroring in progress [1/2, 0	) bytes] - [clone.whtt]			
File Preferences Mirror Log	Window Help			
	In progress:	Transferring data		
DentestPau	Bytes saved:	08	Links scanned:	1/2
	Transfer rate:		Files undated:	0
Program Filer	Active connections:	2	Errors:	0
Program Files (x86)		-		_
Users	Actions			
E-2 Vipul	scanning https://	//haveibeenpwned.com		SKIP
.anaconda	connect https://	//haveibeenpwned.com/		SKIP
.android				SKIP
.conda				SKIP
.idlerc				SKIP
.ipynb_checkpoi				SKIP
.ipython				SKIP
jupyter				
.VirtualBox				SKIP
				SKIP
				SKIP
🖃 📃 Desktop				SKIP
⊡ 22nd july to :				SKIP
E. Clone				
🕂 🚽 🔒 🔒 🔒				
⊕ hts-cachı		< Back	Next>	Cancel Help
cookies.t				
hts-log.b				

#### Step 20: Finally click on Finish to complete the Task.

Site mirroring finished! - [Clone.whtt	]
File Preferences Mirror Log Wi	ndow Help
Local Disk <c:> </c:>	Mirroring operation complete. Click Exit to quit WinHTTrack. See log file(s) if necessary to ensure that everything is OK. Thanks for using WinHTTrack! Tip: Click [View log file] to see warning or error messages
Users Public Vipul anaconda android .android .android .conda .idlerc .ipython .ipython .jupyter .VirtualBox .VirtualBox .VirtualBox .Contacts .Contacts .Desktop	View log file         Browse Mirrored Website         < Back

Step 21: Following folders will be created by HTtrack in the end.



# **Introduction to CURL**

Curl is small computer utility which is used for transferringdata from various protocols.

Libs curl is a free client-side URL transfer library.

It support cookies, HTTP, HTTP/2, FTP and Gopher etc.

It also performs SSL certificate verification.

## Steps to Run Curl

Step 1 To connect and fetch the data just write this command in terminal of kali.



# Step 2 Here it is showing the result of the command i.e. curlmodernindianbabynames.com



#### Step 3 Result continue..



Step 4 Command if user want to send particular request by using different http method.



Step 5 Here it is showing the result of the command i.e. curl -v - X HEAD modernindianbabynames.com

root@kali: ~	•	8
File Edit View Search Terminal Help		
<pre>root@kali:~# curl -v -X HEAD modernindianbabynames.com Warning: Setting custom HTTP method to HEAD with -X/request may not work Warning: way you want. Consider using -I/head instead. * Rebuilt URL to: modernindianbabynames.com/ * Trying 195.201.169.48 * TCP_NODELAY set</pre>	the	Â
<pre>* Connected to modernindianbabynames.com (195.201.169.48) port 80 (#0) &gt; HEAD / HTTP/1.1 &gt; Host: modernindianbabynames.com &gt; User-Agent: curl/7.55.1 &gt; Accept: */*</pre>		
> < HTTP/1.1 200 OK < Date: Fri. 16 Oct 2020 04:52:09 GMT		
< Server: Apache		
< X-Powered-By: PHP/7.2.22 < Access-Control-Allow-Origin: * < Content-Type: text/html; charset=UTF-8		
* no chunk, no close, no size. Assume close to signal end <		
		~

Step 6 To check the redirection we use the command i.e. curl google.com

	root@kali: ~	0	•	0
File Edit View Search Terminal Help				
<b>root@kali</b> :~# curl google.com				*

Step 7 Here the result of the command 301 and 301 Moved means it is redirected.



Step 8 To get the details of redirected website we use the command i.e. curl –L google.com



## Step 9 Here it is showing the result of the command

<pre>Fig Edit Vew Sexts Termed Hep Fig Edit Vew Sexts Termed Fig Fig Vex Sexts Termed Fig PopPing Edit Vex Carbon Fig PopPing Fig Fig PopPing Fig PopP</pre>	Applications   Places   Terminal	Fri 00:53	1 🗯 💉 🕬 🙂 🗸
<pre>Text bit row forst finded integ Text bit row forst finded</pre>		root@kall: ~	
<pre>rodegum:=r curl - L google.com </pre>	File Edit View Search Terminal Help		
<pre>Var a=window.location,b=a.href.indexOf("#");if(0&lt;=b){var c=a.href.substring(b+1);/(" b)q=/.test(c)&amp;b-1=<c.indexof("#")&ba.replace(" search"+c.replace(")<br="">/(^ b)fp=[^b]*/g,"")+"scadeh");<style>bfgbar,#guser{font-size:l3px;padding-top:lapx limportant;}#gbar{height:22px}#guser{padding-bottom:7px !im portant;text-align:right].gbh,.gbd{border-top:lap solid #c9d7f1;font-size:l3px;padding-top:lapx limportant;}#gbar{height:22px}#guser{padding-bottom:7px !im portant;text-align:right].gbh{.gbd{border-top:lapx solid #c9d7f1;font-size:l3px}gbh{height:0;position:absolute;top:24px;width:100%}@media all{.gbl{height :22px;margin-right:.5em;vertical-align:top}#gbar{float:left]}a.gbl,a.gb4{text-decoration:underline !important}a.gbl,a.gb4{color:#00c !important}.gbi . gb4{color:#dd8e27 !important}.gbf .gb4{color:#900 !important} </style><style>body,td,a,p,.hfdfont-family:arial,sans-serif}body{margin:0;overflow-y:scroll}#gog{padding:3px 8px 0}td{line-height:.8em}.gac_m td{line-he ight:17px}form{margin-bottom:20px}.h{color:#36c}.q{color:#00c}em{font-weight:bold;font-style:normal}.lst{height:25px;width:496px}.gsfi, .lst{font:18px a rial,sans-serif}.gsfs{font:17px arial,sans-serif}.ds{display:inline-box;display;inline-block;margin:3px 0 4px;margin-left:4px}input{font-family:inherit }body{background:#fff;color:#000}a{color:#11c;text-decoration:none}a:hover,a:active{text-decoration:underline}.fl a{color:#51a8b} sblc{padding-top:5px}.sblc addisplay:block;margin:2px 0;margin:0 12px}.lsb{background:#eee;border:solid 1px;border-color:#ccc #999 #999 #ccc;height:30px}.lsb{display:block;#wargin:0;outline:0;font:15px arial,sans-serif;vertical-align:top}.lsb-active{background:#ccc}.lst:focu s{outline:none}</pre></td><td><pre>raot@katl:-# curl -L google.com </pre> </pre> <pre>cldoctype html><html itemscope="" itemtype="http://scl Type">smeta content="/images/branding/googleg/lx/googl SbitdQ==">(function(){window.google={kEI: 'VSeJX47Aud ,5,1128,56,170,648,3226,226,314,3,65,985,283,868,112,4, 188,8384,4859,1361,9290,3028,3890,850,11033,1808,4020, ,149,1103,840,519,1521,157,4100,312,1132,4,3,2063,666 4,642,7877,4928,108,3407,908,2,941,2614,2397,7468,170 1860,445,1948,74,1436,281,52,214,2163,463,460,1555,400 19,912,564,681,8,430,31,1303,2551,139,3094,874,116,52, 798,40,171,605,2,44,837,409,314,413,11,686,45,42,22,9] 8,57,275,632,1093,838,835,2,362,39,98,71,69,196,505,90 (390,886,1,9,2,2551,1,748,141,59,736,563,1,4265,1,1,2) google.sn='webhp';google.kHt='en-IN';})();(function()) te("eid")));)a=a,parentNode;return ( google.kEI;googl Node;return c);google.logt=lrunction(a,c,b,d,g) (%dd=google.gettEI(d)&&(e=*Gkiei=*d));d=**;16&&googl atyp=i&ct=*a+&cad=*c+e+f*&zx=*+google.time()+d;/^1);return b};}).call(this);(function(){google.tm}={unction(a,google.tm}); gle.loadAll=function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.logu=function(a}{google.tm}; function(a,b){google.tm}=function(a}{google.tm}; function(a,b){google.tm}=function(a}{google.tm}; function(a,b){google.tm}=function(a}{google.tm}; function(a,b){google.tm}=function(a}{google.tm}; function(a,b){google.tm}=function(a}{google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; function(a,b){google.tm}; fu</td><td><pre>mema.org/WebPage" lang="en-IN"><head><meta content="text/html; eeg_standard_color_128dp.png" itemprop="image"><title>Google</ idd_EPtryXuAO', kEXPI: '0.202162,1151585,5662,730,224,5105,206,3 553,319,414,129,7,855,1683,7,222,90,1116857,1197776,507,328984 978,7931,5297,2054,920,873,10622,1141,7512,5874,4518,1398,137 2023,1777,143,377,1947,2229,93,328,1284,16,2927,2246,1813,178 7,1035,1316,3,2108,175,997,1426,69,305,1728,582,1514,603,2,44 1774,1256,255,2214,849,82,1374,638,146,521,827,130,360,115,2, 7,240,7,257,113,143,42,26,13,23,1785,114,2267,528,752,151,693, 1021,9,305,3299,248,595,11,951,17,30,2,23,3,51,127,39,31,12,6, google.lc=[];google.li=0;google.getEI=function(a){for(var c;a le.getEI=function(a){for(var c=null;a&&(!a.getAttribute  !(c le.time=function(%cshid=")&&%shid==%d&(=*shid="+g e.cshid&===c.search("&cshid=")&&%shid==%d&(=*shid="+g e.cshid&===c.search("&cshid=")&&%shid==%d&(=*shid="+g e.cshid&===c.search("&cshid=")&&%shid==%d&(=*shid="+g e.cshid&=herc.search("&cshid=")&&%shid==%d&(=*shid="+g the;i.tes(tb)&&"https:"==window.location.protocl&&(google.teshid="+goog http:/i.tes(tb)&&"https:"==window.location.protocl&&(google.to();wh n.push.apply(google.lma);google.lq=];google.load=function(a) l(thi);google.f={};(function(){ ction(b){ar a;if(a=b.target}{ar = "= =.getAttribute("data-subm stopPropagation());wh);d(a)var =="ae.getAttribute("data-subm stopPropagation());wh);d(a)var =""==a.getAttribute("data-nohref"</td><td>charset=UTF-8" http-equiv="Content- title><script nonce="yAl0KgzqT/meGZi 204,10,1226,364,1499,612,205,383,246 ,13677,4855,32691,16115,19397,9287,9 9,919,2278,7,2796,1593,1279,2212,536 7,3227,1990,856,6,4774,1294,6286,445 24,4,1528,2304,217,1019,271,874,405, 0,252,1753,509,1968,3036,870,1,335,5 567,3802,611,37,954,756,613,55,744,3 125,478,25,624,54,103,70,144,2,1,3,7 5996993,2801217,549,333,444,12,10,3,7 5996993,2801217,549,333,444,12,80,1 23959151,2716137,17691',KBL:'2A20'}; &&(1a.getAttribute[]!(c=a.getAttribu =a.getAttribute[]!(c=a.getAttribu =a.getAttribute[]!(c=a.getAttribu =a.getAttribute[]!(c=a.getAttribu =b,d,g]{if(b=google.logUr(la,c,b,d,g google.vel.lu&&google.vel.lu(b);a.sr oogle.getEI(d),-1=c.search("&lei=") le.cshid);b=b=]"/"(+[G] "gen_2C4")+"" (lError("a"),!1,{src:b,glmm:1}),b="" ile(google.l[c])}google.y[c]=a,b];r ,b,c]google.l=1==c[]"q"==c&Gla.eleme ner("click",function(b){var a;a:{for );break a}=!la&&b.preventDefault()</td></tr><tr><td><pre>gev[coto:moto:/immoto:/immoto:moto:moto:moto:moto:moto:moto:mot</td><td><pre>var a=window.location,b=a.href.indexOf("#");if(0<=b){ /(^ &)fp=[^&]*/g, "")+"&cad=h")};</script><style>#gbar portant;text-align:right).gbh,.gbd{border-top:lpx sol t:22px;margin-right:.5em;vertical-align:top}#gbar{floc phd{color:#dd827 !!mopctant}.ghf _mb4(color:#000 !!mm</pre></td><td><pre>var c=a.href.substring(b+1);/(^\&)q=/.test(c)&&-1==c.indexOf(" #guser{font-size:13px;padding-top:1px !important;}#gbar{heigh .d #c9d7f1;font-size:1px}.gbh{height:0;position:absolute;top:2 it:left}a.gbla.gb4{text-decoration:underline !important}a.gb portant}</pre></td><td>#")&&a.replace("/search?"+c.replace( t:22px}#guser{padding-bottom:7px !im 4px;width:100%}@media all{.gbl{heigh 1,a.gb4{color:#00c !important}.gbi .</td></tr><tr><td></td><td>gowtector.woodc2/ important;gor .gowtector:#366 im, </style>scyle&gt;body,td,a,p,.h{font-family:rarial,sans- ight:17px}form{margin-bottom:20px}.h{color:#36c}.q{col rial,sans-serif}.dsfs{font:17px arial,sans-serif}.ds{ }body{background:#fff;color:#000}a{color:#11c;text-de .sblc{padding-top:5px}.sblc a{display:block;margin:2px #999 #ccc;height:30px}.lsbb{display:block}#WqQANb a{di order:none;color:#000;cursor:pointer;height:30px;margi s{outline:none}<script nonce="vAlQKgzqT/me6Zig&lt;/td&gt;&lt;td&gt;&lt;pre&gt;bottent;&lt;br&gt;serif}bodd{margin:0;overflow-y:scroll}#gog{padding:3px 8px 0}t&lt;br&gt;.or:#00c}em{font-weight:bold;font-style:normal}.lst{height:25p&lt;br&gt;lisplay:inline-box;display:inline-block;margin:3px 0 4px;margi&lt;br&gt;:oration:none}a:hover,a:active{text-decoration:underline}.fl a&lt;br&gt;( 0;margin-left:13px;font-size:11px}.lsbb{background:#eee;bord&lt;br&gt;.splay:inline-block;margin:0 12px}.lsb{background:unl(/images/&lt;br&gt;.n:0;outline:0;font:15px arial,sans-serif;vertical-align:top}.&lt;br&gt;ibitdzQ=="></script></c.indexof("#")&ba.replace("></pre>			

#### Step 10 We use this command to save the websites HTML Content.

Applications ▼ Places ▼ ▷ Terminal ▼	Fri 00:54
	root@kali: ~
File Edit View Search Terminal Help	
<pre>root@kali:~# curl -o curl.txt modernindianbabynames.com</pre>	
	20
	38

Step 11 Result of the command showing total 29859 files saved.

Applications 👻	Places 🔻 🕟 Te	erminal 👻						Fri 00:54	
								root@kali: ~	
File Edit View	Search Terminal	Help							
root@kali:~#	curl -o cı	ırl.txt	modernir	dianbabyn	ames.com				
% Total	% Received	% Xfe	rd Avera	ge Speed	Time	Time	Time	Current	
			Dload	Upload	Total	Spent	Left	Speed	
100 29859	0 29859	Θ	0 29859	) 0 -	-::	::	::-	- 35004	
<pre>root@kali:~#</pre>									

Step 12 To view the details of downloaded files use the command vim curl.txt

Applications   Places   I. Terminal	Fri 00:55	1 🗯 💉 🕪 🕛 🔻
	curl.txt (~) - VIM	000
File Edit View Search Terminal Help		
<pre><!DOCTYPE html>    </pre>		
<pre><?if IF 8?><html class="ie ie8"> <?endif]-</pre></html></pre>		
<![if IE 9?> <html class="ie ie9"> <?endif]-</td><td></td><td></td></html>		
<![if gt IE 9?> <html lang="en"> <!--</td--><td><?endif?></td><td></td></html>	endif?	
<head></head>		
Basic		
<meta charset="utf-8"/>		
<title>Modern Indian Baby Names</title>		
<meta content="Modern India&lt;/td&gt;&lt;td&gt;n Baby Names - The largest Database of most beautiful and modern Hindu, Muslim, Arabi&lt;/td&gt;&lt;td&gt;c, Sikh, Bengali, En&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;glish, American, Baby Boy and Girl Names along&lt;/td&gt;&lt;td&gt;with meanings and search options." name="Description"/>		
<pre><meta content="Modern, Most, Most&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;odren, Beautiful, Meaningful, Meaning, Hindi, Hindu, Indian, Muslim, Arabic, English,&lt;/td&gt;&lt;td&gt;American, Unique, U&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;necxceptional, Unusual, Topmost, Frequently Us&lt;/td&gt;&lt;td&gt;ed, Sikh, Bengali, Telugu, Sindhi, Punjabi, Kudi, Girl, Boy, Beta Beti, UnCommon, Bab&lt;/td&gt;&lt;td&gt;y, Names, Babyname,&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Babynames, Namkaran, Namimg, A, Baby,in, India&lt;/td&gt;&lt;td&gt;" name="Keywords"/></pre>		
<link <="" href="/images/favicon" rel="shortcut icon" td=""/> <td>n.ico" type="image/x-icon"/&gt;</td> <td></td>	n.ico" type="image/x-icon"/>	
<pre><base href="https://www.modernindianbabynames.&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;com/"/></pre>		
<pre><meta content="width=device-width=de&lt;/td&gt;&lt;td&gt;dth,initial-scale=1.0,user-scalable=yes" name="viewport"/></pre>		
<pre><link css="" file<br="" fonts.googleapis.com="" nref="nttps://fonts.googleapis.com/css/file&lt;br&gt;link href=" nttps:=""/>link href="nttps://fonts.googleapis.com/css/file link href="nttps://fonts.google</pre>	amily=upen+Sans:300,400,600,700,800 Snadows+into+Lignt" ret="stylesneet" type="text/c	SS">
<pre><link etulophoet"="" href="https://eduio.alog&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;amily=concert+one" nrer="nttps://fonts.googleapis.com/css/file&lt;br&gt;link nal=" ret="stylesneet"/></pre>		
<pre><link href="/theme/css/ie css&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;[[endif]&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;![if lte IE 8]&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;&lt;script src=" nrel="nttps://cdnjs.clo&lt;br&gt;&lt;/td&gt;&lt;td&gt;uditare.com/ajax/tibs/iont-awesome/4./.u/css/iont-awesome.min.css &gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;&lt;li&gt;k Hood Libs&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;AINGLANDADYNAMES.COM/CSS/CUSIOM.CSS /&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;&lt;pre&gt;circle for the second secon&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;&lt;script site /js/modernizi.js //script/&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;&lt;li&gt;clink rel=" rel="stylesheet" respond.is"="" stylesheet"="" theme="" vendor=""/></pre>	t>	
endif?		
<pre><script <="" async="" pre="" src="https://securepubads.g.doub"></td><td><pre>leclick.net/tag/js/gpt.js"></script></pre>		
<script></script>		