

# **INSTITUTE OF AERONAUTICAL ENGINEERING**

(Autonomous) Dundigal - 500 043, Hyderabad, Telangana

## **COURSE CONTENT**

# PENETRATION TESTING AND CYBER OPERATIONS LABORATORY

**VI Semester:** CSE(CS) **Course Code** Category Hours / Week Credits **Maximum Marks** L Р С CIA SEE Total Т ACCC10 CORE 0 2 2 70 1 30 100 **Tutorial Classes: Nil Practical Classes: 33 Total Classes: 45 Contact Classes: 12 Prerequisite:** Network security

### I. COURSE OVERVIEW:

The purpose of this course is to provide a clear understanding of assessing an application or infrastructure for vulnerabilities in an attempt to exploit those vulnerabilities, and circumvent or defeat security features of system components through rigorous manual testing.

#### **II. COURSES OBJECTIVES:**

#### The students will try to

#### learn

- I. The tools that can be used to perform information gathering.
- II. The Various attacks in various domains of cyberspace.
- III. How vulnerability assessment can be carried out by means of automatic tools or manual investigation.
- IV. The vulnerabilities associated with various network applications and database system.

### **III. COURSE OUTCOMES:**

#### At the end of the course students should be able to:

- CO 1 Make use of Google and Whois tools to gather information about the target specification.
- CO 2 Apply appropriate tools to encrypt and decrypt passwords in network.
- CO 3 Make Use of Nessus tool to identify vulnerabilities and monitor the networking mechanism.
- CO 4 Compare different OSINT tools to detailed network information of the target.
- CO 5 Make use of Virus Total tool to scan the network and detect malware on the network.
- CO 6 Apply Ettercap tool to scan the network and performing an ARP poisoning attack.

# EXERCISES FOR PENETRATION TESTING AND CYBER OPERATIONS LABORATORY

**Note:** Students are encouraged to bring their own laptops for laboratory practice sessions.

# **1. Getting Started with** Understanding of scanning and reconnaissance process.

# **Introduction:**

A penetration test, colloquially known as a pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system. Penetration tests usually simulate a variety of attacks that could threaten a business. They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system.

# **Softwares used:**

Osint Tools Vulnerability Tools Attack detection Tools Encryption Tools

# 1.1 Scanning any of the target with domain name

To Perform Scanning of the target we need to understand all scanning types as shown in below

There are different types of scans available

Syntax: Nmap domain name

Example: nmap www.amazon.com

### Type of scan: Regular

👁 Zenmap		
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> e	łp	
Target: www.amazon.com	n 🗸 Prof	le: Regular scan
Command: nmap www.a	mazon.com	Intense scan
		Intense scan plus UDP
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	Intense scan, all TCP ports
OS 4 Host	nmap www.amazon.com	Intense scan, no ping
Www.amazon.com	Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-08 10:54 India Standard Time	Ping scan
Www.amazon.com	Nmap scan report for www.amazon.com (100.15/.24/.131) Host is up (0.017s latency).	Quick scan
	rDNS record for 108.157.247.131: server-108-157-247-131.hyd57.r.cloudfront.net	Quick scan plus
	PORT STATE SERVICE	Quick traceroute
	21/tcp open ftp 25/tcp open smtp	Regular scan
	80/tcp open http	Slow comprehensive scan
	143/tcp open imap	
	443/tcp open https	
	465/tcp closed Smtps 587/tcp open submission	
	6346/tcp closed gnutella	
	New Area 4 Th address (4 best on) areas 4 to 47 47 and	

### Try

Students can use different types of scans to perform on the target.

### Hint

Select type of scan from Nmap tool on target.

# 1.2 Scanning any of the target with IP Address

Perform Scanning of the target we need to understand all scanning types as shown in below There are different types of scans available

Syntax: Nmap IP Address

Example: nmap 108.157.247.131

#### Type of scan: Regular

### Output:

👁 Zenmap	
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> elp	p
Target: 108.157.247.131	V Profile: Regular scan
Command: nmap 108.157.	247.131
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans
OS 4 Host	nmap 108.157.247.131
3 www.amazon.com	<pre>Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-08 11:02 India Standard Time Nmap scan report for server-108-157-247-131.hyd57.r.cloudfront.net (108.157.247.131) Host is up (0.011s latency). Not shown: 991 filtered tcp ports (no-response) PORT STATE SERVICE 21/tcp open ftp 25/tcp open smtp 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open https 587/tcp closed smtps 587/tcp closed smtps 1 IP address (1 host up) scanned in 16.28 seconds</pre>

### Try

Students should perform scanning of the target with variety of scan types as shown in above.

#### Hint:

Select the type of scan from dropdown window appeared on screen

# 2. Use Google and Whois for Reconnaissance to gather information about target.

Open-Source Intelligence (OSINT) is the collection, analysis, and dissemination of information that is publicly available and legally accessible. Right now, OSINT is used by a organizations, including governments, businesses, and non-governmental organizations.

### Step1: open Google Step2: Type Whois on google WHOIS Search, Domain Name, Website, and IP Tools - Who.is

https://wh	<b>o.is</b> /whois/iare.a	c.in							# A 10 3
who.i	Search for do	omains or IP addresses	٩	Premium Domain	s Transfer	Features	Login	Sign Up	
		Interested in	n domain names? <u>Clic</u>	k here to stay up to date	e with domain nan	ne news and pro	motions a	at Name.com	
			iare.ac.in is a	already registere	d. Interested in b	uying it? Make a	ın Offer		
	.ac.in	.com	.net	.org	.CO \$245.00	.i \$34	<b>D</b> .99	<b>.app</b> \$16.99	.live
	Taken	Taken	Taken	Taken	Available	Avail	able	Available	Taken
iare, whois inf	.ac.in formation DNS Record	is Diagnostics							
Simila	ır Domains						Use p	romo code WHOIS to : Name.com	save 15% on your first order.
iare.ac.ir iare.in   i	n   iare.art   iare.bi are.info   iare.it   i	iz   iare.cn   iare.co.in iare.net   iare.nu   iare	iare.co.uk   iare.com .one   iare.online   iare	iare.com.br   iare.com e.org   iare.org.il	.tr   iare.digital   ia	re.edu		Find the perfect de	omain at
Regis	trar Data			We will display store	ed WHOIS data for u	p to 30 days. rivate Now	Ex	verythin	σ

#### Step3: check DNS Records

Internation Whois DNS Records Diagnostics									
DNS Records	DNS Records for iare.ac.in cache expires in 3 minutes and 49 sec								
Hostname	Туре	TTL	Priority	Content					
iare.ac.in	SOA	3600		ns4.ctrls.in hostmaster@ctrls.in 2023030113 28800 7200 1209600 3600					
iare.ac.in	NS	3600		ns4.ctrls.in					
iare.ac.in	NS	3600		ns5.ctrls.in					
iare.ac.in	А	3600		137.59.201.77					
iare.ac.in	MX	3600	5	alt1.aspmx.l.google.com					
iare.ac.in	MX	3600	1	aspmx.l.google.com					
iare.ac.in	MX	3600	5	alt2.aspmx.l.google.com					
iare.ac.in	MX	3600	10	alt3.aspmx.l.google.com					
iare.ac.in	MX	3600	10	alt4.aspmx.l.google.com					
www.iare.ac.in	А	3600		137.59.201.77					
www.iare.ac.in	CNAME	3600		lare.ac.in					
www.iare.ac.in	MX	3600	1	aspmx.l.google.com					



## Try:

Use other OSINT tools to gather information to find information of target network.

#### Hint:

Use Google Dorks, Babel X as a OSINT tools

# 3. Make use of Crypt tool for Encryption and decryption procedure

### 3.1 Install Crypt tool

#### Software Requirements:

- Supported operating systems:
- Windows 10/11/ Linux
- 64-bit OS X/macOS 10.6 or later

**Step1:** Download and install crypt tool **Step2:** open software

Ç <sub>Î</sub>	example-en	
Sta	xample for the CrypTool version family 1.x (CT1)	
Ren		
The	essor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than C	T1. In C
0		
abo	r (CTT) is a comprehensive and free educational program	
offer	tensive online help and many visualizations.	
This	Ste was excepted in order to halo you to make your first stone with CT4	
This	ile was created in order to help you to make your first steps with CTT.	
1) T The Pres	rting page of the online help offers the best oversight of CT1's capacity. From the starting page you can rea ng page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main to start the online help everywhere in CT1.	ch all e n windo
2) A	ible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/D	ecrypt
3) T	re several examples (tutorials) within the online help which provide an easy way to gain an understanding o	fcrypto
4) Y	n further develop your knowledge by:	
- Na	ig playfully through the menus. You can press F1 at any selected menu item to get more information.	
- Re	the included readme file (see the menu "Help -> Readme").	ofthio
- Vi	the webpage www.cryptool.org.	or this

Step 4: enter data to encrypt and decrypt file Step 5: select any of algorithm to encrypt

Eil	e j	<u>E</u> dit	<u>V</u> iew I	En <u>c</u> rypt/Decrypt	Digital Signatures/ <u>P</u> KI	Indiv. Procedures	<u>A</u> nalysis	<u>O</u> ptions	<u>W</u> indow	<u>H</u> elp				
	)   c	2 🖬		) 🔏 🖻 🖻	3 ⊞ ? №									
	۵.													
		carting	example	e-en										
	SU	<b>XT</b> Սո	named1											
F	Re	xzzvo	dsvdsvd	svdbvdsvdsv										
	"													
	Cr													
	off													
	n I													
	1) Th													
F	Pr							K	ey Entry: IDE	:A				×
	2)								Enter the ke	y using hexadecim	al characters (09,	AF).		
									Key length:	128 bits	•			
ľ	"									0 00 00 00	00 00 00 00	00 00 00 00	00.00	200
4	4)											,		0
H	F													
	Ì								Encryp	٤	Decrypt	t	Car	ncel

**Step6:** based on selection of algorithm enter password **Step 7:** again, open file to decrypt

🖉 🖆		
starting	igexample-en	
t 👷 Ur	Innamed1	
,e 🚾 🧧	🚰 RC4 encryption of <unnamed1>, key &lt;23&gt;</unnamed1>	
h     [	00000000 21 17 EB B3 2F 66 99 E4 34 63 FF 3B 8B AF 24 E1 DC FD 9C 65 79 99	!∕f4c.;\$ey.
ff		
h		
6		
2		
F		
h		

**Step8:** enter the password to decrypt **Step9:** file will be decrypted

#### Try:

Use different cryptographic algorithms for perform encrypt and decrypt procedure **Hint:** 

use symmetric modern algorithms like IDEA, RC2, RC4

use symmetric classic algorithms like Caesar, Hill, substitution algoriths

# 4. Install Password Cracking tool Cain and able to Crack the password

# 4.1 installing Cain and able Tool

### Requirements

The actual version requires the following items:

10Mb Hard-Disk space-

Microsoft Windows 2000/XP/2003/Vista-

Winpcap Packet Driver (v2.3 or above; AirPcap adapter is supported from Winpcap version 4.0).

### Setup

Just run the Self-Installing executable package and follow the installation instructions.

The package will copy all the files needed by the program into the installation directory.

### **Installation Files**

Cain's setup program will install and/or replace these files in your system:

- Cain.exe [the main executable program]
- Cain.exe.sig [author's PGP signature of the file Cain.exe]
- CA\_UserManual.chm [this file]
- Abel.exe [the executable of the Windows service named Abel ]

- Abel.exe.sig [author's PGP signature of the file Abel.exe]
- Abel.dll [a DLL file needed by the program]- Abel.dll.sig [author's PGP signature of the file Abel.dll]
- Uninstal.exe [the uninstallation program]
- Wordlist.txt [a little word list file]
- Install.log [the log file of the installation package, you can check everything modified on your system here]
- Whatsnew.txt [contains differences between versions]
- oui.txt [a list file that contains vendor's information about MAC addresses]
- <Installation Dir>\winrtgen\winrtgen.exe [Winrtgen a windows utility to generate Rainbow Tables]
- <Installation Dir>\winrtgen\winrtgen.exe.sig [author's PGP signature of the file winrtgen.exe]

- <Installation Dir>\winrtgen\charset.txt [an example file containing charset definitions for winrtgen.exe and Cain's cryptanalysisattacks]

- <Installation Dir>\Driver\WinPcap\_4\_1\_beta5.exe [the original distribution package of the Winpcap drivers] All the above files will be installed in the Installation directory and subdirectories.

### **Abel Installation**

Abel is a Windows NT service composed of two files: "Abel.exe" and "Abel.dll".

These files are copied by the installation packageinto the program's directory but the service is NOT automatically installed on the system.

Abel can be installed locally or remotely (using Cain) and requires Administrator's privileges on the target machine.

### LOCAL INSTALLATION:

1) Copy the files Abel.exe and Abel.dll into the %WINNT% directory (E.G.: C:\WINNT or C:\Windows)

- 2) Launch Abel.exe to install the service (it is not automatically started)
- 3) Start the service using the Windows Service Manager (services.msc)

### **REMOTE INSTALLATION:**

- 1) Use the "Network TAB" in Cain and choose the target remote computer where you want to install Abel
- 2) Right click on the computer icon in the left tree and select "Connect As"
- 3) Provide Administrator's credentials for the remote system
- 4) Once connected right click on the "Services" icon and select the menu entry "Install Abel"
- 5) That's it! The two files 'Abel.exe' and 'Abel.dll' will automatically be copied to the remote machine's root directory i.e. C:\winnt,C:\Windows); the service will automatically be installed and started.

## 4.2 Dictionary attack

Dictionary attack uses a predetermined list of words from a dictionary to generate possible passwords that may match the MD5 encrypted password. This is one of the easiest andquickest way to obtain any given password.

Start Cain & Abel via the Desktop Shortcut 'Cain' or Start menu. (Start > Programs > Cain > Cain). Choose 'Yes' to proceed when a 'User Account Control' notification pops up regarding software authorization.

Once on, select the 'Cracker' tab with the key symbol, then click on MD5 Hashes. The result should look like the image below.

🙎 Decoders	🔮 Network	🙀 Sniffer 🕑	Cracker 🧟 Tracerou	ute 🔝 CCD
Cracker		MD5 Hash	Password	Note
EM & NTLM	Hashes (			
MTLMv2 Ha	ashes (0)			
MS-Cache I	Hashes (I			
🛞 PWL files (I	0)			
Cisco IOS-I	MD5 Hast			
Cisco PIX-N	1D5 Hast			
APOP-MD5	Hashes (			
CRAM-MD5	6 Hashes			
OSPF-MD5	Hashes (			
+ RIPv2-MD5	6 Hashes			
VRRP-HMA	C Hashes			
VNC-3DES	(0)			
MD2 Hashe	es (0)			
MD4 Hashe	es (0)	-		
MD5 Hashe	es (0)			
T SHA-1 Has	hes (U)			
SHA SHA-2 Has	hes (0)			
	STATE AND	-		

1. As you might have noticed we don't have any passwords to crack, thus for the next few steps we will create our own MD5 encrypted passwords. First, locate the Hash Calculator among a row of icons near the top. Open it.

P <sub>64</sub> 🕙 📶 🖼	R 🚾 🖬	🖸 😵 💋	0 ?	i
Traceroute	CCDU	Wireless	D Quer	y ]

2. Next, type into 'Text to Hash' the word password. It will generate a list of hashes pertaining to different types of hash algorithms. We will be focusing on MD5 hash so copy it. Then exit calculator by clicking 'Cancel' (Fun Fact: Hashes are case sensitive so any slight changes to the text will change the hashes generated, try changing a letter or two and you will see. This is called the avalanche effect.)

ash Calculator	
<ul> <li>Text to hash</li> </ul>	
password	
C Bytes to has	h (HEX)
т Туре	Hash 🔄
MD2	F03881A88C6E 391 35F0E CC60EFD 609B9
MD4	RA9D09951458701DE177328288189C74
105	SPANOTE ACOUSTIC FOR THE CONTRACT CONTR
3HA-2 (256) 3HA-2 (384) 3HA-2 (512) 3HPEMD-160 M M VT MySQL323 MySQL323 MySQL323 MySQL3HA1 Cisco PIX VNC Hash Base64	56894699024204715100556790C532773630006A48B0D62411E772101542C A8864484D0ACA14589B07576184210475882820034784D6A751258E64598 B109F38B6C244E84241917E006D18B9005D098938EFD185E07394C706A88E 2008E97898475A9799F57342C5380B25FF31 E52CAC574193942 B464F7AE6E9F8117A0068D03387586C 50213939C58F67 24700C0050E42F016188B99005A0C42EC901E19 NuLK-W46g45HEK0 D8B83CF0727A1459 c6Fz344cmQ=
•[	• •
	Calculate Cancel

- After you exit, right click and select 'Add to list', paste your hash then click OK. Your first encrypted password! But don't stop there, add the following MD5 hashes from the words PaSS, 13579, 15473, sunshine89, and c@t69.
- 4. With all the encrypted MD5 passwords on hand, we can finally start! Move your cursor and select all **six passwords**, then right click and press **'Dictionary Attack'**.
- 5. Once the window opens, go up to the dictionary and select 'Wordlist.txt', right click and select 'Reset initial file position'. You'll know you've resetted when there's nothing under the position column. Note: Make sure to do this every time you want to restart dictionary attack!

ile		Position	
C:\Program Files\Cain\Wordlists\Wordlig	Add to list	Insert	1
	Change initial f	ile position	
	Reset initial file	position	
	Resectar Inicial	nie posicions	
ey Rate	Remove from li	st	

9.Click **'start'** and watch the magic happens before your eyes! Once it ends **'exit'**. Your result should be the same as below.

Plaintext Plaintext Plaintext Attack sto 3 of 6 has	of of of shes	E13DD027BE0F2152( 5F4DCC3B5AA765D6; F3C33935E245CE33( d! cracked	CE387AC0EA83D8 1D8327DEB882CF CE9AF31C3D5624	63 is 99 is 80 is	13579 password sunshine89	

### Try:

Apply different cracking methods to crack the passwords.

### Hint:

Rain bow tables, Brute force Attacks methods can use for crack passwords.

# 5. Find the Vulnerabilities of the target using Nmap tool.

We can use and apply variety of commands on Nmap tool to find the vulnerabilities on target network.

#### Cmd: nmap -sV --script vulners www.bookmyshow.com



nmap -sV --script vuln www.bookmyshow.com

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 14:14 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.46.182)
Host is up (0.0048s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.49.182 104.16.48.182 104.16.45.182 104.16.47.182
Not shown: 989 filtered tcp ports (no-response)
PORT
        STATE SERVICE VERSION
21/tcp open ftp?
25/tcp open smtp
smtp-vuln-cve2010-4344:
   The SMTP server is not Exim: NOT VULNERABLE
fingerprint-strings:
   GenericLines:
     220 Sophos ESMTP ready
     unrecognized command
     unrecognized command
   Hello:
     220 Sophos ESMTP ready
     Syntactically invalid EHLO argument(s)
   Help:
     220 Sophos ESMTP ready
      214-Commands supported:
     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
    NULL:
     220 Sophos ESMTP ready
80/tcp open http
                        Cloudflare http proxy
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
_http-csrf: Couldn't find any CSRF vulnerabilities.
_http-dombased-xss: Couldn't find any DOM based XSS.
_http-passwd: ERROR: Script execution failed (use -d to debug)
http-server-header: cloudflare
110/tcp open pop3?
_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
__sslv2-drown: ERROR: Script execution failed (use -d to debug)
 _tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
__ssl-dh-params: ERROR: Script execution failed (use -d to debug)
 _ssl-heartbleed: ERROR: Script execution failed (use -d to debug)
|_ssl-cert-intaddr: ERROR: Script execution failed (use -d to debug)
 _ssl-ccs-injection: ERROR: Script execution failed (use -d to debug)
_ssl-poodle: ERROR: Script execution failed (use -d to debug)
143/tcp open imap?
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
_sslv2-drown: ERROR: Script execution failed (use -d to debug)
```

# 5.1 using csrf as NSE script

http-csrf: Cross-Site Request Forgery (CSRF)

vulnerabilities are detected by this script.

nmap -sV --script http-csrf www.bookmyshow.com

Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 14:23 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.45.182)
Host is up (0.0048s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.46.182 104.16.48.182 104.16.49.182 104.16.47.182
Not shown: 989 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp?
25/tcp open smtp
fingerprint-strings:
GenericLines:
220 Sophos ESMTP ready
unrecognized command
unrecognized command
Hello:
220 Sophos ESMTP ready
Syntactically invalid EHLO argument(s)
Help:
220 Sophos ESMTP ready
214-Commands supported:
AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
NULL:
220 Sophos ESMTP ready
80/tcp open http Cloudflare http proxy
_http-server-header: cloudflare
_http-csrf: Couldn't find any CSRF vulnerabilities.
110/tcp open pop3?
143/tcp open imap?
443/tcp open ssl/http Cloudflare http proxy
http-server-header: cloudflare
_http-csrf: Couldn't find any CSRF vulnerabilities.
465/tcp closed smtps
587/tcp open smtp
fingerprint-strings:

# 5.2 using password

Attempts to retrieve /etc/passwd or boot.ini to see if a web server is vulnerable to directory traversal.

nmap -sV --script http-passwd www.bookmyshow.com



### Try:

Use slowloris command to check vulnerabilities on target **Hint:** 

nmap -sV --script http-slowloris-check www.bookmyshow.com

# 6. Analyze web application digital history of the target address using Way back Machine tool.

# **Use Wayback Machine Tool**

**Way back** Machine is an online tool for maintaining of digital library (internet achieve) of web application, captured records of previous data related to different types of web applications.

# **Steps for Analyzing:**

- **1.**Open Way back machine tool in online
- 2. After opening it on online displays like this,

← C ▲ Not secure   web.archive.org	A* to C   t= te
🔟 INTERNET 🗃 WEB 💷 BOOKS 💾 VIDEO 🎖 AUDIO 🎴 SOFTWARE 🕼 IMAGES	SIGN UP   LOG IN 🛧 ÚPLOAD 🔍 Search
ABOUT BLOG PROJECTS HELP DONATE 💗 CONTAC	T JOBS VOLUNTEER PEOPLE
DONATE UNTERNET ARCHIVE Explore more than 800 billion	web pages saved over time d to a site's home page

- 3.Type URL or target on search box.
- 4.the fallowing information will be displayed about target.



5. See the data in different ways mentioned in the diagram

- Calendar wise
- Collections wise
- Changes wise
- Summery wise
- Site Map wise
- URLs wise
- •

Ex: In the calendar wise we can observe each and every captured record on particular day of month Select any of the day and displays what time it has been captured also



**6.** Click on the type wise as mentioned above to see the information of target Suppose I can click on summary wise I can see the information in fallowing way.



## Try:

Find the information of target that updated on URL's wise

## Hint:

Use URLs information then click on URLs or Explore target URLs that displays URL's information of target

# 7. Download and install Nessus tool in windows operating system, to run Vulnerability Scan with Nessus tool

## 7.1 Download and Install Nessus.

- Download Nessus from the Tenable Downloads site.
- When we download Nessus, ensure the package selected is specific to your operating system and
- processor. There is a single Nessus package per operating system and processor. Nessus Manager, Nessus Professional, and Nessus Expert do not have different packages; your activation code determines which Nessus product is installed.

## **Start Nessus Installation:**

- 1. Navigate to the folder where you downloaded the Nessus installer.
- 2. Next, double-click the file name to start the installation process.

## Complete the Windows InstallShield Wizard with the fallowing steps

- 1. First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue.
- 2. On the **License Agreement** screen, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.
- 3. Select the I accept the terms of the license agreement option, and then click Next.
- 4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder.
- 5. On the Ready to Install the Program screen, select the Install button.

The **Installing Tenable**, **Inc. Nessus** screen appears and a **Status** indication bar shows the installation progress. The process may take several minutes.

After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser.

# To access a locally installed Nessus instance, go to https://localhost:8834. Perform the remaining Nessus installation steps (Adding plug-ins) in your web browser.

# 7.2 Run Your First Vulnerability Scan with Nessus tool.

## Step 1: Creating a Scan

Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan:

In the top navigation bar, click Scans. In the upper-right corner of the My Scans page, click the New Scan button.



# Step 2: Choose a Scan Template

Scanner				
6	, <b>C</b> I	na the second	F.	\$
Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.	Advanced Scan Configure a scan without using any recommendations.	Audit Cloud Infrastructure Audit the configuration of third- party cloud services.	Badlock Detection Remote and local checks for CVE- 2016-2118 and CVE-2016-0128.	Bash Shellshock Detection Remote and local checks for CVE- 2014-6271 and CVE-2014-7169.
M	R		6	
Basic Network Can A full system scan suitable for any host.	Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	DROWN Detection Remote checks for CVE-2016-0800.	Host Discovery A simple scan to discover live hosts and open ports.	Intel AMT Security Bypass Remote and local checks for CVE- 2017-5689.
The state	Q	<b>•</b>		
	Malware Scan	MDM Config Audit	Mobile Device Scan	Offline Config Audit

- Next, click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set. For a detailed explanation of all the options available, refer to Scan and Policy Settings in the Nessus User Guide.
- A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see Create a Policy in the Nessus User Guide.
- The Nessus interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of Nessus Professional.
- To see a full list of the types of templates available in Nessus, see Scan and Policy Templates. To quickly get started with Nessus, use the Basic Network Scan template.

# **Step 3: Configure Scan Settings**

Prepare your scan by configuring the settings available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

# Follow these steps to run a basic scan:

**1. Configure the settings in the Basic Settings section.** 

Nessus 🔊	Scans Settings		
Houses	New Scan / Basic Ne * Back to Scan Templates	etwork Scan	
All Scans	Settings Credentials	Plugins 👁	
	BASIC ~	General Settings	
D Policies	* General	Niama.	and a second
Plugin Rules	Schedule	rearrie	
Customized Reports	Notifications	Description	
G Scanners	DISCOVERY		
	ASSESSMENT		
	REPORT , Folder	Folder	My Scins
	ADVANCED >	Tamatu	
		Upload Targets Post-Processing	Add FRe
	Save • Cancel	Uve Results Enabling this option will	dentify jotential issues discovered by plugies added during spdatus—without actively scarving targets.

# The following are Basic settings:

Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the Nessus interface.
Description	(Optional) Specifies a description of the scan or policy.
Folder	Specifies the folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

# 2. Configure remaining settings

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

# **3. Configure Credentials**

Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.

Nessus	Scans Settings		🧧 TestUser 🛃
My Scans	New Scan / Basic Network S « Back to Scan Templates	Scan	
All Scans	Settings Credentials Plugin	n =	
	CATEGORIES Hest		
O Policies			
Plugin Rules     Customized Reports	55H		
👙 Scanners	Windows	()	

# 4. Launch Scan

- After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.
- If you want to launch the scan immediately, click the down button, and then click Launch. Launching the scan will also save it.
- The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

# **Step 4: Viewing Your Results**

Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.

# You can view scan results in one of several views:

Page	Description
Hosts	Displays all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity.
Remediations	If the scan's results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.
Notes	Displays additional information about the scan and the scan's results.
History	Displays a list of scans: Start Time, End Time, and the Scan Statuses.

## Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

asic Network Back to My Scans			Co	onfigure	Audit Trail	Launch 💌	Export	6
Hosts 1 Vulnerabilities 66 Rem	ediations 2 History 1							
Filter   Search Vulnerabilities  Q	66 Vulnerabilities							
Sev - Name	Family	Count		Φ.	Scan Details			
CRITICAL Jenkins < 2.46.2 / 2.57 and Je	. CGI abuses	1		1	Name: Status:	Basic Network		
CRITICAL MS17-010: Security Update f	Windows	1		1	Policy:	Basic Network Scan		
Jenkins < 2.121.2 / 2.133 Mul	CGI abuses	1		1	Start:	February 25 at 9:03	AM	
Jenkins < 2.138.4 LTS / 2.150	CGI abuses	1		1	Elapsed:	4 minutes		
Jenkins < 2.150.2 LTS / 2.160	CGI abuses	1		1	Vulnerabilitie	15		
MS12-020: Vulnerabilities in	Windows	1		1		Critica		
Jenkins < 2.107.2 / 2.116 Mul	. CGI abuses	1		1		Mediu Low	m	
Jenkins < 2.121.3 / 2.138 Mul	. CGI abuses	1		1		• Info		
Jenkins < 2.138.2 / 2.146 Mul	. CGI abuses	1		1				
Jenkins < 2.73.3 / 2.89 Multip	. CGI abuses	1		1				
MEDIUM Jenkins < 2.89.2 / 2.95 Multip	. CGI abuses	1		1				
Jenkins < 2.89.4 / 2.107 Multi	. CGI abuses	1		1				
Microsoft Windows Remote	Windows	1		1				

## To view vulnerabilities:

In the top navigation bar, click Scans.

- Click the scan for which you want to view results.
- Do one of the following:
- Click a specific host to view vulnerabilities found on that host.
- Click the Vulnerabilities tab to view all vulnerabilities.
- (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.

• Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.

	> Vulnerabilities 27	
мерим	crosoft Windows SMB NULL Session Authentication	Plugin Details
Description		Severity: Medium
he remote host is ru	inning Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).	ID: 26920
	· · · · · · · · · · · · · · · · · · ·	Type: remote
Repending on the co	infiguration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.	Family: Windows
		Published: 2007/10/04
Solution		Modified: 2012/02/29
Apply the following r	egistry changes per the referenced Technet advisories :	
		Risk Information
HKLM/SYSTEM/Cur	rentControlSet/ControlLSA/RestrictAnonymouse 1	And Annaly and Annaly
HKLM\SYSTEM\Cur	rentControlSet\Services\Janmanserver/parameters\restrictnullsessaccess=1	NISK Factor: Medium CVSS Base Scorer 5.0
		CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/EN/A:N
<ul> <li>HKLM/SYSTEM/Cur</li> </ul>	om : rentControlSet/Services/Janmanserver/parameters/NullSessionPipes	CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
		CVSS Temporal Score: 4.3
leboot once the reg	istry changes are complete.	
		Vulnerability Information
iee Also		Exploit Available: fake
http://support.micro	soft.com/kb/q143474/	Exploit Ease: No known exploits are available
http://support.micro	ioft.com/kb/q246261/	Vulnerability Pub Date: 1999/07/14
mpy/ween/technicros	na en	
Dutput		Reference Information
It was possibl	le to bind to the \browser pipe	CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-
Port *	Hosts	OSVD8: 299, 8230
THE OWNER AND		8(D: 494

### **Step 5: Reporting Your Results**

Scan results can be exported in several file formats.

### To Export a Scan Report:

- Start from a scan's results page
- In the upper-right corner, click Export.
- From the drop-down box, select the format in which you want to export the scan results.
- Click Export to download the report.

#### Try:

Find Vulnerabilities based on Host discovery content

#### Hint:

Select the option from menu as "Host discovery content" and choose the target

# 8. Install Acunetix tool to understand and perform scanning for variety of vulnerabilities in web application.

### 8.1 Install Acunetix tool

Step1: go to the location to find the official URL of Acunetix tool as mentioned below Acunetix Web Vulnerability Scanner 11.0 Download (Free trial)... (informer.com)

Step2: after downloading it double click on application file.



**Step3:** perform sequence of steps to complete the process of installation.

In the installation process application asking you to set administrative user account mentioned below

n s	Setup - Acunetix 11 Trial	—		$\times$
•	Administrative User Set administrative user			*
	To access Acunetix scanning interface you need an administra Please enter login information here. Email	itive user a	ccount.	
	Password			
	Confirm password			
	< Back	<u>N</u> ext >	) <b>Ca</b>	ncel

- **Step 4:** mention username and password
- Step 5: server port default it is taken, else customize if you want
- **Step 6:** complete and finish the process has been completed
- **Step 7:** after completion of installation

$\leftarrow$	C	Ô	https://localhost:13443/#/login/			
				acunetix	WEB APPLICATION SECURITY	
				Si	gn In	
				Email This field is required		•
				Password		
				Keep me signed in		
				Copyright © 2017 Acunetix Ltd.	www.acunetix.com	

**Step 8:** enter mail Id and password to log on to the application page After enter the page displays as fallows

~	C 🗈 https://	cahost13443/#/ 🖉 A 🏠 🤆 🛱 🌘 🖤 …	b
•	acunetix		
	3	Scan Add Target Delete Add to Group Generate Report WAF Export •	Filter
æ	Dashboard	No Targets created yet. Create new Target	
0	Targets		
ŵ	Vulnerabilities		
-	Scans		
Б	Reports		
۰	Settings		

**Step 9:** check all the options for knowledge of each and every option **Step 10:** click on Targets

In targets click on Add target or Create new Target as fallows

	Add Target	×	
an Add Target Delete	Address		
<b>:ts created yet.</b> Create new Target	http://example.com/		
	Description		
	Add Ta	arget Close	

Step 11: after adding the target the page displays like this

······································	< Back	Scan	Save						
Dashboard	General	Crawl	нттр	Advanced					
Targets									
Vulnerabilities			Target I	nfo					
Scans					https://www	/.flickr.com/			
Reports				Description	just for finding vulr	nerabilities			
Settings				Business Criticality	Normal			-	
				Scan Speed	Slower	Slow	Moderate	Fast	
				Continuous Scanning					

**Step 12:** click on Scan and there types will be displayed

Keneral Crawl HTTP	Scan Type	Full Scan	~	
	Adva Report	None	•	
	Schedule	Instant	•	
			1 scan will be created	
			Create Scan Close	
	Business Critica	lity Normal		-

Step 13: choose the type which u want to perform scan as mentioned below

Scan Type	Full Scan		•
Report	Full Scan		
	High Risk Vulnerabilities		
Schedule	Cross-site Scripting Vulnerabilities		
	SQL Injection Vulnerabilities		
	Weak Passwords		
	Crawl Only		
		Create Scan	Close

**Step 14:** after mention the type and schedule scan instant click on create scan. After clicking on that the page displays as fallows

а	Back Stop Scan Generate Report WAF Exp	iort •		
Dashboard	Scan Stats & Info Vulnerabilities Site Structure	Events		
<ul> <li>Targets</li> </ul>				
🕅 Vulnerabilities			Activity	Processing
A Scane	Acunetix Threat Leve	el	Overall progress	0%
Scans	Threat level is not available	e yet.	Scanning of user flickr com started	Mar 16, 2023 5-19-08 PM
🖹 Reports			· commy or minimum concorrigation	NUL 20, 2020 012000 TH
Settings				
	Scan Duration	Requests	Avg. Response Time	Locations
	1m 5s	452	1,115ms	1,256
	Target Information		Latest Alerts	
	Address	www.flickr.com	No vulnerabilities detected	
	Server	Unknown		
	Operating System	Unknown		

In the above we can see scan start and stop options, vulnerabilities, site structure, events **Step 15:** wait till the process of scanning completed

Step 16: after completed generate the report for scanned results.

**Step 17:** after generated download the report of scanned results.

By default, the report downloaded in PDF format as mentioned below with scanned results

Scan details		
Scan information		
Start time		16/03/2023, 15:50:37
Start url		https://www.iare.ac.in/
Host		https://www.iare.ac.in/
Scan time		6 minutes, 34 seconds
Profile		Cross-site Scripting Vulnerabilities
Acunetix Threat Level	0	
Acunetix Threat Level No vulnerabilities have b Alerts distribution	0 ween discovered by the sca	inner.
Acunetix Threat Level No vulnerabilities have b Alerts distribution Total alerts found	0 eeen discovered by the sca	inner.
Acunetix Threat Level No vulnerabilities have b Nerts distribution Total alerts found High	0 eeen discovered by the sca 0 0	inner.
Acunetix Threat Level No vulnerabilities have b Nerts distribution Total alerts found High Medium	0 eeen discovered by the sca 0 0 0	inner.
Acunetix Threat Level No vulnerabilities have b Nerts distribution Total alerts found High Medium Low	0 eeen discovered by the sca 0 0 0 0 0	inner.

### Try:

Use type of scan High Risk Vulnerabilities to find the target vulnerabilities

### Hint:

Select the scan type from scans as Highrisk vulnerability category

# 9. Perform ARP Poisoning on target network.

- 1. **Open three virtual machines :** In this you shall require a Kali 2.0 VM (we'll call this VM1), and two more VM's running operating systems Windows 7/8/8.1/10 (VM2 and VM3)
- 2. On all 3 virtual machines, go to settings and make sure that the network adapter is set to NAT. This is important, you cannot set it to bridge or host only, it must be NAT. This is for all 3 machines.
- 3. On VM1, open terminal and run "ifconfig". On VM2 and VM3, open up cmd and run "ipconfig". Take note of your IP address and MAC address on each of the respective machines. 4. On VM3, go on the Internet and download a windows application XAMP. Download version "7.0.4 / PHP 7.0.4" under XAMPP for Windows on this page: <u>https://www.apachefriends.org/download.html</u>
- 4. Install XAMP using the downloaded installer file. Don not change any settings or check/uncheck any boxes. Just keep pressing "next" until you finish.
- 5. Once done installation, run XAMPP Control Panel on VM3. Once the main window pops up, start the Apache server by pressing he Start button on the Apache module row.
- 6. To test the server, go on the internet on VM2 and type in http://. It should display a generic welcome page that looks like the following:



 If successful, now go to VM1 (reminder – the one running Kali Linux 2.0. Arnold's should have the credentials root/toor). Go to applications and select "Applications > 09 – Sniffing & Spoofing > ettercap-graphical".



6. Go to Sniff > Unified Sniffing OR Pres Shift+U

File	Sniff Options ?		etterc	ap 0.8.0	
	Unified sniffing	Shift+U	< =		
	Bridged sniffing	Shift+B	-		
	Set pcap filter	Р	~		
-	7	E	t	t	e

7. Select interface eth0

-		attancan In				
	~	accercap in	puc			
4	Network interf	ace : et	nO		~ <b>–</b>	
	V	_				
			ок	Cance		
Ļ						
11.	. Click Hosts > Scan fo	or hosts				
:s	Hosts View Mitm	Filters	Logging	Plugins	?	
_	Hosts list	н				
1	Scan for bosts	Ctrl+S				
	Load from file	Ctrl+0		-		
£	Save to file	Ctrl+S	-			
· · ·	Stark -					
	P The second	1				
1						
-						

12.Click Hosts > Hosts List



13. From the new tab that appeared, you will see a list of IP's. Add the IP of VM3 to target #1 and add the IP of VM2 to target #2.



14. Go to Mitm > Arp Poisoning. In the pop up window that appears, only check "sniff remote connections" and press OK

						e	ettercap	0.8.0			
	Start	Targets	Hosts	View	Mitm	Filters	Logging	Plugin	s P	_	
	Host I	List 🛛			Arp	poisonin	g	<			
	IP Ad	ldress	MAC	Addres	lcmp Port	o redirec stealing	t				
	192.1	L68.56.1	08:00	0:27:00	Dhc	p spoofir	ng				
	192.1	168.56.10	2 08:00	0:27:79	Stop	o mitm at	tack(s)				
15. Click on Start > S	Start	Sniffing					_	_			
			5t	Target Start sniffin Stop sniffin Exit 92.168.56.1	s Hosts g Ctr g Ct Ct 100 08:0	View M t+W trl+E p0:027:F5:C6 00:27:79:20	litm Filters Descrip 4:93 5:29 C:92	ettercap O. Logging	.8.0 Plugins		

- 16. Now go to "Applications > 09 Sniffing & Spoofing > wireshark"
- 17. Select eth0 and start scan
- 18. Now type in "arp" in the filters to only retrieve arp messages. Take note of the MAC addresses compared to the IP's. Also take note of the frequency of said messages
- 19. Now go to VM2 and repeat Step 7
- 20. Go back to VM1 and now type in a filter "ip.src==&&http" to get all http requests to server. You should notice there being 2 HTTP requests sent from VM2 to VM3. However, take note of the MAC addresses. One of the requests should go from VM2 to VM1 and the next should go to from VM1 to VM3. If this is the case, you know we see a successful ARP poisoning.
- 21. Repeat step 20, just flip make VM3 the source IP and analyze all HTTP responses outgoing from the server. Similar idea, there should be two one going from VM3 to VM1 and another going from

VM1 to VM2, but both in the name of VM3 to VM2 in the sniffed packets frame. 22. Congrats, you now know how to successfully ARP poison

# 10. Performing security testing of web applications using Burp Suite toolkit.

**Step 2:** Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.

PortSv		Besearch Academy Daily Swin Support Y
	Burn Suite Enterprise Edition	Dat Burn Suite Cartified
	The enterprise enterprise exiting scanner.	Prove your skills with the world's leading pentesting toolkit.
	Burp Suite Professional The world's #1 web penetration testing toolkit.	
	Burp Suite Community Edition The best manual loois to start web security testing.	Central patenticate

**Step 3:** New webpage will open, which will ask for email id, and other option is Go Straight to downloads. Click on Go straight to downloads.



**Step 4:** After clicking on Go straight to downloads new webpage will open which will contain two versions of burp suite one is Burp suite community edition and the other is burp suite professional along with compatibility for different operating systems.

Stable	ommunity 202	21.10.5			
02 December 2021 at 15:14 UTC				🔰 🕓 🗗 🍯 in 💟	
Burp Suite Community Edition	✓ Windows (64-bit)	v	Download	show checksums	
Burp Suite Professional					
Burp Suite Community Edition	well as several minor bug fixes	i.			
rofessional / Cor	nmunity 202	1.10.3			
				🔰 🖸 🖬 🍲	in
rp Suite Community Edition	Windows (64-bit)	~	Download	show checksums	
s release provides a security patch, as w	JAR Linux (64-bit)				

**Step 5:** Choose Burp suite Community Edition along with Windows (64-bit). Click on the download button, downloading of the executable file will start shortly. It is a big 210 MB file that will take some time depending on download speed.

	portswigger.net/burp/releases/protessional-community-2021-10-3/requestededition=community	6 章	*
ps G	, umai 🖬 toullude 🔮 Maps 🥕 pymon requests oo 🔮 index of /receate/ 🖷 NCLEN 🔓 box animation - yo 👂 kanks Aggregation 💪 lord shiva tunko po	**	LE Re
	Burp Suite Releases	a sale	
		9	
	Professional / Community 2021 10.2		
	Professional / Community 2021.10.3		
	20 December 2021 at 15:14 UTG		
	🔰 🖸 🖬	in 🔤	
	Burp Suite Community Edition Vindows (64-bit) Vindows (64-bit) Download Show checksums		
	This release exception a security match, as well as accurate piper have		
	This telease provides a security parcin, as were as several minior bug likes.		
	Security patch		
	Security patch		
	Security patcn We have fixed a medium-severity security issue in the way Burp Suite processed HTTP/2 responses, which could have introduced XSS in certain circumstances.		

**Step 6:** Now check for the executable file in downloads in your system and run it. **Step 7:** Loading of Installation Wizard will appear which will take a few seconds



Step 8: After this Setup screen will appear, click on Next.



**Step 9:** The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.

Setup - Burp Suite	Community Edition	on 2021.10.3			~
Select Destination Where should Bur	Directory p Suite Commun	ity Edition be installe	ed?	-	<
Select the folder wh then click Next.	ere you would lik	ce Burp Suite Comm	unity <mark>Edition t</mark>	o be instal <mark>l</mark> ed	-
C:\Users\Dell\App	Data\Local\Prog	rams\BurpSuiteCom	munity	Browse	. )
Required disk space	: 294 MB				
Free unix space					
		< Back	Next >	Can	cel

**Step 10:** Next screen will be of choosing Start menu folder so don't do anything just click on Next Button.

Setup - Burp Suite Community Edition 2021.10.3	
Select Start Menu Folder	
Where should Setup place the program's shortcuts?	
Select the Start Menu folder in which you would like Setup to cr shortcuts, then click Next.	eate the program's
Burp Suite Community Edition	
Accessories	
Administrative Tools	
Adobe	
AnyDesk	
Flex Windows	
Free Cam 8	
Games	
Intel PROSet Wireless	
Internet Download Manager	
< Back	Next > Cancel

**Step 11:** After this installation process will start and will hardly take a minute to complete the installation.



# Step 12: Click on Finish after the installation process is complete.



Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop.



Step 14: Run the software, screen containing terms and conditions will appear Click on I Accept.

Please read the second	ne following t erms.	terms and con	ditions careful	ly, and indicate	e whether you
Burp Suite Co	ommunity Edit	tion Terms and	Conditions o	f Supply	1
IMPORTANT I DOWNLOAD	NOTICE: PLEAS	E READ THE FO WARE FROM T SOFTWARE.	HIS WEBSITE,	AS APPLICABLE	RDERING OR TO THE
These Burp S documents re PortSwigger software com or the "Softw	uite Commun ferred to in it Ltd ("Licensor" prising Burp are"), followir	ity Terms and o t ("Terms") cons ") will grant to Suite Commun og acceptance	Conditions of stitute the terr any user ("Lice nity Edition ("B of an order as	Supply togeth ns and conditions nsee") a licence urp Suite Com detailed belo	er with the ons on which e to use the munity Edition <sup>*</sup> w.
The following	g expressly for	rm part of the ty Licence Agre	ement;		
		-			

**Step 15:** New screen containing information regarding the project will appear, choose temporary project and click Next.

Burp Suite Community Edition v20	21.10.3		
Welcome to Burp Suite Commu project.     Note Disk-based projects are only	nity Edition. Use i	the options below to create o Suite Professional	Community Edition
<ul> <li>New project on disk</li> </ul>	Namei Filei		Choose file
Open existing project		Name	File
	File		Choose file
		Pause Automated Tasks	Cancel Next

**Step 16:** Next screen is about using default settings or loading from configuration file, click on Use Burp Defaults.

S Burp Suite Community Edition v2021.10.3	— <b>—</b> ×
Select the configuration that you would like	I load for this project.
O Use Burp defaults	
Use options saved with project	
Load from configuration file	File
File:	Choose file
Default to the above in future	
Disable extensions	
	Cancel Back Start Burp

**Step 17:** Project will start loading.

Burp Suite Community Edition v2021.10.3	×
	Burp Suite
	Starting project, please wait
-	Cancel

**Step 18:** Finally new project window will appear.

rp Suite Community Editio	n v2021.10.3 - Terr	porary Project		-							- 0 ×
Project Intruder Rej hboard Target P	roxy Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn	
arn, explore and d	iscover										[Hide this tab]
Getting started w	th Burp Suite				-	0	Burp	Suite - a guide	d video tour		
Get going right away - wit	h our quick start tu	torial.		-	15	1	Take a r features Wate	un-through of all the	: major Burp Suite		
Burp Suite video tuto	rials			-		-	The W	eb Security Acade	imy		
See how to use Burp Suite tools.	's main features an	d				-	Learn h- Suite.	ow to find more vuln learning	erabilities using Bu	p	
Burp Suite Support Co	nter						Burp S	uite on Twitter			-
Find the answers to your I here.	Surp Suite question	5		(			Join Bur know.	p Suite's huge comm	iunity, and stay in th	ne	
Find answers							Follo	w us			-

# **Process for performing security testing:**

- Open Burp suite application on your desktop / Laptop
- By default, selected as "Temporary project" for project selection
- Click on next
- Use by default "burp defaults"
- Click on start burp
- Now burp suite Project window displays as fallows

Dashboard Target Proxy Intru	ier Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Extension	15			,
Tasks	🕒 New	scan 🔘 New I	ve task (II	) © © ⊮*	comparer	Time	to level up? C	atch more	b Update is r	ady to install	
Fitter Running Paused Finished	Live task Scan	Intruder attack	,P fee	orch	Issue ac	tivity [Pro	version only	1	Restart 8	Later	More info
1. Live passive crawl from Proxy (all traffic)				001	V Filter	High M	edium Low	Info	Certain Fi	m Tentative	P Search
Add links. Add item Helf, same domain and URLs in sulte scope. O Remi added to site map O responses processed O responses queued				Issue type         Hot         Path           * supplication input transformation perfect         http://inscure-ban         /uls-hoten           * supplication insude         http://inscure-ban         /uls-hoten           * Supplication insude         http://inscure-ban         /uls-hoten           * Oran Hader methy section         http://inscure-ban         /uls-hoten           * Oran Hader methy section         http://inscure-ban         /inscure-ban           * Oran Hader methy section         http://inscure-ban, /uls-hotespation         http://inscure-ban, /uls-hotespation           * Oran Lasteria service interaction OHTP         http://inscure-ban, /uls-hotespation         http://inscure-ban, /uls-hotespation           * Scill prefixion         http://inscure-ban, /ulse-hotespation         http://inscure-ban, /ulse-hotespation           * Scill prefixion         http://inscure-ban, /ulse-hotespation         http://inscure-ban, /ulse-hotespation           * Scill prefixion         http://inscure-ban, /ulse-hotespation         http://inscure-ban, /ulse-hotespation			Path				
Event log				@ «"	Advisory						
Filter Critical Error (Into Debug)			,Q _5e	sich_							
Time ∨ Type Source 12:50:07.9 May 2023 Error Proxy Faile	d to start proxy serv	Message ice on 127.0.0.1:808	) - Check wheth	er another 🗹							

- Open "proxy" tab on menu
- Check "intercept" is on / off
- If intercept is "off" make it as "on"
- Check proxy with proxy address
- As fallows in browser proxy settings.

	Certificate verification problem dete $\times$	18 Settings	× +		
_	→ C 🔹	Firefox about:preferences	s		
	C     C	Browsing Use gutoscrollin Use smooth so Show a touch is Always use the Search for text Enable picture- Control media Recommend is Recommend is	Connection Settings  Connecti	Port         8081           Pgrt         8081           Port         0           Reload	
	2 Extensions & Themes	Network Setti	o proxy for	DK Cancel	

- Once intercept is "on"
- Go to the target menu
- Open any browser
- After open browser event log will be recorded.
- Give any target
- Record the response as shown in below

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Extensions
Intercept	HTTP histor	y Web	Sockets history	(2)	Proxy settings					
Reques	t to https://w	ww.google	.com:443 [142.2	50.195.164]						
Forward		Drop	Intercept is	s on	Action	Open browser	1			
Pretty Ra	W Hex									
GET /sear	ch?q=iare.	acin&o	q=iare.aci	in&gs_lcr	p=EgZjaHJvbWUy	BggAEEUY0dIBC	DQ10TNqMGo3	qAIAsAIA&sou	rceid=chro	me&ie=UTF-8 HTT
Host: www	.google.co	>m.								
Sec-Ch-Ua	: "Not:A-B	Srand";v=	"99", "Chron	nium";v="	112"					
Sec-Ch-Ua	-Mobile:									
Sec-Ch-Ua	-Platform	"Window	/s "							
Upgrade-1	nsecure-Re	equests:	1							
User-Ager	t: Mozilla	1/5.0 (Wi	ndows NT 10.	.0; Win64	; x64) AppleWe	bKit/537.36 (	KHTML, like	Gecko) Chro	me/112.0.5	615.50 Safari/5
Accept:										
text/html	,applicat:	on/xhtml	+xml, applica	ation/xml	;q=0.9,image/a	wif,image/web	p,image/apn	g,*/*;q=0.8,	applicatio	n/signed-exchan
X-Client-	Data: CJa	)YwE=								
) Sec-Fetch	-Site: nor	le								
Sec-Fetch	-Mode: nat	<i>r</i> igate								
Sec-Fetch	-User: 71									
Sec-Fetch	-Dest: doo	rument								
Accept-Er	coding: g	ip, defl	ate							
Accept-La	inguage: er	n-US,en;q	1=0.9							
Connectio	n: close									

Check and observe all the menus for different responses based on different targets



# Try:

Use Collaborator, Sequencer to find the issues on activity of target

# Hint:

Click on the menu's called Collaborator and Sequencer, perform scans the issues for report.

# 11. Install and Perform Web Applications Testing On Attacks Using Owasp Zap Tool

11.1 Owasp Zap Installation process

Step1: go to the official site of OWASP ZAP and visit downloads on site as shown in below

OWASP ZAP – Download (zaproxy.org)

Step2: click on download by choosing the operating system

Step3: after downloaded tool in your system double click on that setup file

Step4: click on next



**Step5:** accept the terms and conditions and click on next

8	🔇 Setup - OWASP Zed Attack Proxy 2.12.0	-		$\times$
I	License Agreement Please read the following important information before	continuing.		
F	Please read the following License Agreement. You must a agreement before continuing with the installation.	ccept the terms	s of this	
	Apache License Version 2.0, January 2004 http://www.apache.org/licenses/			
	TERMS AND CONDITIONS FOR USE, REPRODUCTION,	AND DISTRIBU	JTION	
	1. Definitions.			
(	I accept the agreement     I do not accept the agreement			
inst	nstall4j			
	< Back	Next >	Ca	ncel

Step6: choose installation type "standard" and click on "next"



Step7: installation process being started and displays finish window once it is completed



Step 8: click on finish to complete installation.

# 11.2 Perform Web application testing Automated

After installation of OWASP ZED open it on your system as shown in below



Click on automated scan to perform the scanning of web application

Untitled Session - 20230511-170141 - OWASP ZAP 2.12.0	
File Edit View Analyse Report Tools Import Export Online Help	
Standard Mode 🖂 🗋 🔚 📰 🚔 🚔 🔐 🚅 🛤 📰 🥅 🗐	i i i i i i i i i i i i i i i i i i i
😂 Sites 🕂	🗧 🐓 Quick Start 🖈 🗯 Request 🗰 Response 🔗 Requester 🛛 🛨
e - · · · ·	
Contexts	Automated Scan
Default Context	
v 🙆 Stes	This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
<ul> <li>https://lirefox.settings.services.mozilla.com</li> </ul>	Please he suggest that you should only attack applications that you have been seen it ally been alway permission to test
> P v1	
https://shavar.services.mozila.com	
https://location.services.mozilla.com	URL to attack: Ditro Server internation
> a https://www.jntua.ac.in	
> iii n http://www.jntua.ac.in	Use traditional spider.
	Use ajax spider: with Firefox ~
	F Attack Stop
	Progress: Using traditional solder to discover the content
	ropess. Calify another an experience are consent
🗯 History 🔍 Search  Pe Alerts 📄 Output 👾 Spider 🖈 🔺 🦒 Act	ive Scan 📲
₩ New Scan Progress: 1: http://www.jntua.ac.in > 11	15% 💞 Current Scans: 1 URLs Found: 1429 Nodes Added: 63 🦷 Export
URLs Added Nodes Messages	
Processed Reg Timestamp	101 Code Reason BTT Size-Rean Mander Size-Rean Rody Michael Alart
E(11/2) E-12-40 EM GET Miter (Ausser johus	a latitudes and admission courses 200 CM2 200 mm 200 bates 52 500 bates
5/11/23, 5:13:49 PM GET https://www.intua.	c.n/mtua-doa-ph-d-admissions-under 200 OK 440 ms 339 bytes 52,535 bytes
6/11/23, 5:13:49 PM GET https://www.jntua.	ac.in/timetables-for-b-pharm-iv-yr-i-se 200 OK 204 ms 339 bytes 52,497 bytes
6/11/23, 5:13:49 PM GET https://www.jntua.	ac.in/ph-d-full-time-programme-2022-2. 200 OK 471 ms 339 bytes 63,083 bytes
6/11/23, 5:13:49 PM GET https://www.jntua.	ac.in/ph-d-full-time-programs-at-intua-c 200 OK 298 ms 339 bytes 52,237 bytes
<ul> <li>b/11/23, b/13/49 PM GET https://www.jntua.</li> <li>b/14/23, b/13/49 PM GET https://www.jntua.</li> </ul>	ac.mappic.ation=hor-sponsored-seats- zuv UN, zvir ms 339 bytes 52,453 bytes to iorzteo-sentretoriese/ 200 CVC 424 ppc 292 bytes 81 132 bytes
<ul> <li>GET Hugs//www.jitua.</li> </ul>	active government and the active sector of the sector of t

During scanning of the process just pause the scan process and right click on any url to see content To see content rightclick on URL and select "open URL in browser" as shown in below

•	Results of MCA I & II sem Reg & × +		~ -			
$\leftarrow \rightarrow c$	🐵 🔿 🛔 https:/	/www.jntua.ac.in/results-of-mca-i-ii-sem-reg-supple-dec-jan-2018-19-exams-circular-from-ce-pgdt-17-04 🗉 🏠	8	ව එ		
Thursday 11	th May 2023	Contact Us   Anti-Ragg	ng Toll Free No: 1800	0 425 27:		
e-Maga	Jawaharlal Nehru Technological University Anantapur Us: Construction of the stabilished under A.P. Govt. Act No.30 of 2008) Ananthapuramu - 515002, Andhra Pradesh, India. e-Magazine April 2023 Issue   75 Years Celebrations of JNTUACEA-Videos  JNTUA Anthem   AP EAPCET 2022   MORTH Recruitment   AP PGCET 2023   Azar ka Amrit Mahotsa					
kaspers		1. FDP on Artifi	cial Intellig	kas		
	Genesis- JNTUA Chancellor	Administration Directorates Programs Offered Constituent Units Our Faculty e-Mag	azine			
	ation Reports NIRF AISHE	Contact Us		<		
	evance Portal	Results of MCA I & II sem Reg & Supple Dec/Jan 2018/19 Exams – Circular 17.04.2019	from CE (P			
		Download				
		MCA I & II sem results circular				

After completing scanning, it shows the history of scanned results Generate the reports as shown in below



# Try:

Perform web application testing In manual mode using Owasp Zap

# Hint:

Select the option in manual for any target and perform web application testing.

# 12. Install meta sploit framework tool to perform various exploitation tasks about the security vulnerabilities of a target machine

# 12.1 Installation of Metasploit framework

**Step1:** To install Metasploit framework tool go to official site <u>https://www.metasploit.com/</u> and Click on download

**Step2:** it is redirected to github page and click on nightly installer.html file

**Step3:** again it is redirected to <u>https://docs.metasploit.com/docs/using-metasploit/getting-</u> <u>started/nightly-installers.html</u> this link

**step 4:** in the above link select "latest windows installer" on that page now the setup file will be downloaded.

Step 5: double click on setup file the fallowing page will be displays



**Step 6:** click on "next" and accept terms and conditions on that page, click on next **Step 7:** choose the location to store the installation as shown in below

Metasploit-framework v6.3.16 Setup	– – ×
Custom Setup Select the way you want features to be installed.	
Click the icons in the tree below to change the way	features will be installed.
Metasploit-framework	This feature requires 289MB on your hard drive.
Location: C:\	Browse
Reget Disk Usage	Back Next Cancel

Step 8: click on next and click on install on this page

Metasploit-framework v6.3.16 Setup			$\times$
Ready to install Metasploit-framework v6.3.16		spl	oit
Click Install to begin the installation. Click Back to review or c settings. Click Cancel to exit the wizard.	hange any of your	installation	
Back	🐤 Install	Can	cel

Step 9: now installation process is started as shown in below

Metaspioit-framework vo.3. 16 Setup			~
Installing Metasploit-framework v6	5.3.16	meta frameworl	asploit
Please wait while the Setup Wizard installs Me	etasploit-frame	work v6.3.16.	
Status: Extracting files, please wait			
	Back	Next	Cancel

**Step 10:** after install click on finish to setup has been complete.

(Note: during the installation if any messages u got, we have to do " off" all virus and threat protections on your system)



Now Metasploit framework has been installed on your system.

After installation

Go to the Metasploit frame work folder that installed on your system

**Step 11:** copy the path upto bin folder as like "C:\metasploit-framework\bin"

**Step 12:** set path for installed framework

Step 13: To set the path Edit system environment variables on your PC by right clicking on it.

**Step 14:** Give system variables as "Path" and the value of Path" C:\metasploit-framework\bin" That we copied from installed location

Step 15: Click on Ok to complete the path setup

**Step 16:** now open the command prompt to launch frame work

Type "msfconsole" on command window as shown in below

C:\WINDOWS\system32\cmd. × + ∨
Microsoft Windows [Version 10.0.22621.1555] (c) Microsoft Corporation. All rights reserved.
C:\Users\SLIM 3>cd
C:\Users>cd
C:\>msfconsole C:\metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-core-0.1.30/lib/rex/coi C:metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl nection::Channel::ChannelType::Session::NAME C:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl nection::Channel::ChannelType::Session::NAME C:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl c:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl c:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl C:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl c:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl c:/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rl
dBBBBBBb     dBBBBBP     dBBBBBBP     dBBBBBb     o       'dB'     dB'     BBP       dB'dB'dB'     dBP     dBP       dB'dB'dB'     dBP     dBP       dB'dB'dB'     dBP     dBP
dBBBBBP         dBBBBBb         dBP         dBBBBBP         dBP         dBBBBP         dBP         dBBBBP         dBP         dBBBBP         dBP         dBBBBP         dBP         dBP<
• To boldly go where no shell has gone before
=[metasploit v6.3.16-dev-87ba25c7063076f8e7e47c2c539b20c7544b0e21] +=[ 2314 exploits - 1208 auxiliary - 412 post ] +=[ 972 payLoads - 46 encoders - 11 nops ] +=[ 9 evasion ]

Step 17: to see the commands on Metasploit window just type "help" on window

msf6 > help	
Core Commands	
Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
tips	Show a list of useful productivity tips
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

**Step 18:** type any of the command that you want to see information about that all. **Step 19:** to exit from frame work just type "exit" on screen".

# Try:

Find threads and sessions of the target that using on the same machine.

# Hint:

•

Use Metasploit tool options to find both on target machine.

# 13. Use virus total tool to analyzes files and urls for viruses on target.

13.1 How to use Virus total tool

Intelligence Hunting Graph API

# Step 1: go to virus total official site on online



Step 2: upload any files that you downloaded from internet to find viruses and analysis on it

Step 3: select URL to give target to find viruses or not

Step 4: enter the URL to analyze viruses on files and urls

VIRUSTOTAL						
Analyse suspicious breaches, ai	files, domains, IPs and URLs to detect utomatically share them with the security	malware and other r community.				
FILE	URL	SEARCH	<u> </u>			
www.iare.ac.in						

Step 5: displays all the details related to scanning of the target URL

$\leftarrow$ C	C https://www.virustotal.com/gui/url/6868336664dbd1c2aebf580b3c1df4e7ec9cddc778eb7d51505b63656982ebeb					
ht	tp://www.iare.ac.in/					
		Did you intend to search across the	e file corpus instead? Click here			
	0 0	No security vendors flagged this URL as malicious				
	/ 90 http	//www.iare.ac.in/		200		
	?	v.iare.ac.in		Status		
	DETECTION DETAILS LINKS COMMUNITY					
	Abusix	Clean	Acronis	Clean		
	ADMINUSLabs	⊘ Clean	AICC (MONITORAPP)	🕗 Clean		
	AlienVault	Clean	alphaMountain.ai	🕗 Clean		
	Antiy-AVL	Clean	Artists Against 419	🕑 Clean		
	Avira	Clean	benkow.cc	Clean		
	Bfore.Ai PreCrime	<ul> <li>✓ Clean</li> </ul>	BitDefender	🕑 Clean		

**Step 6:** if any virus detection, then it displays as a count .so from above figure no detection found. **Step 7:** to see details of the target click on details as shown in below

	http://www.lare.ac.in/		
		$\bigcirc$	⊘ No security vendors flagged this URL as malicious
-		00 / 90	http://www.lare.ac.in/ www.lare.ac.in
		Community Score	
		Categories ①	
		Forcepoint ThreatSeeker of Sophos of	ducational institutions
		Xcitium Verdict Cloud r BitDefender e	nedia sharing education
		History O	
		First Submission 2014-04-	10 14:47:42 UTC
		Last Submission 2023-01- Last Analysis 2023-01-	25 13:37:57 UTC 25 13:37:57 UTC
		HTTP Response ①	
		Final URL https://www.iare.ac.in/	
		Serving IP Address 137.59.201.77	
		Status Code 200	
		Body Length 190.16 KB	

**Step 8:** to see links that tool have scanned click on "links" as shown in below

http://www.iare.ac.in/	
	⊘ No security vendors flagged this URL as malicious
/ 90	http://www.iare.ac.in/
Community Score	www.iare.ac.in
DETECTION DET	
Outgoing links 🕁	
https://www.nirfindia.org/	2022/EngineeringRanking.html
https://www.youtube.com	ı/channel/UCrN2YGajq0ITaokeOn2LEpQ
https://mail.google.com	
https://aicte-india.org/fee	dback/
https://www.flickr.com/ph	otos/186282793@N05/albums
https://www.youtube.com	/channel/UCrN2YGajq0ITaokeOn2LEpQ/featured
https://www.facebook.com	n/IAREOFFICIAL
https://twitter.com/@aero	nauticalof
https://www.nirfindia.org/	2022/EngineeringRanking150.html
https://www.ariia.gov.in/H	anking/2021/index.ntmi#divPnarmacyRanking
https://instagram.com/iar	e_nyderabad
https://www.linkedin.com	

**Step 9:** To explore in graph click on "explore" which appears on right corner of window as shown in below

⊘ No security vendors flagged this URL as malicious	Crplote in-
http://www.iare.ac.in/ www.iare.ac.in	200 2023-01-25 13.37:57 UTC Status 3 months ago

Step 10: analyze all details appear on window.

			Disease introduce 3 or more characters to perform a search in the eranh			0
Relation Last serv     Children 1	ing ip addre	55	глава, вномые о от пост славанала по регили на азвеси и вле укруп	Filtered Nodes	0/3	
□ ⊕ ⊙ ♣ Ψ 晶」	. * *	0		Reset all filters Remo	we filtered nodes Remove visible n	nodes
Q 7			URL http://www.iore.oc		Apply to	io selec
Expand				<ul> <li>File Type</li> </ul>		RESET
			(P) 1 act cerving in address	<ul> <li>Entity Type</li> </ul>	ID Address	RESET
No more relationships			(15) Last serving ip a ass	<ul> <li>Relationships</li> </ul>	IP ANNESS OR AND	RESET
Children Relations		28	(S) Network	~ Detections		RESET
Communicating files	3	۸		From To	No detections   With dete	octions
Historical ssl certificates	14	A		0.8 -		
Historical whois	2	Å		0.6 -		
Resolutions	9	Å		0.2 -		
				∘ First Seen		RESET
Relations				From mm/dd/yyyy	To mm/dd/yyyy	8
It doesn't have relations.				1 -		
Show Node List		:=		0.0 -		
				0.4 -		
				0.2 -		
				<ul> <li>Last Seen</li> </ul>		RESET
1				Energy and the second		

Use different target network to analyze suspicious files on target

### Hint:

Give different targets address or IP addresses.

#### V. REFERENCES:

- 1. RafayBaloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 2015.
- 2. Dr. Patrick Engebretson, "The Basics of Hacking and Penetration Testing", Syngress Publications Elseveir, 2013.
- 3. Prakhar Prasad, "Mastering Modern Web Penetration Testing", Packt Publishing, 2016.
- 4. Gilberto Najera Gutierrez, "Kali LinuxWeb Penetration Testing", Cookbook, 2016.
- 5. Robert Svensson, "From Hacking to Report Writing: An Introduction to Security and Penetration Testing", 2016.

#### VI. MATERIALS ONLINE:

- 1. Course Content
- 2. Lab Manual