PROJECT REPORT:

CS 668A: Practical Cyber Security for Cyber Practitioners

Goal: To perform Penetration Testing to find different possible vulnerabilities in various web applications/apps/web services to prepare a finished report for the same as per the observation, and eventually, we will be performing mapping and layer creation using the navigator tool.

By Team SURAKCHA

Yash Uttamchandani (22111070)

Komal Yadav (22111031)

Hrithik Lal (22111027)

LavKush Mani Tripathi (22111034)

Akash Shriwas (22111006)

Mohit Singh (22111402)

Abstract:

Information is a lot of vulnerable than ever; and each technological advance raises new security threat that needs new security solutions. Penetration testing could be a series of activities undertaken to establish and exploit security vulnerabilities. It helps ensure the effectiveness or impotency of the security measures that have been enforced. The Penetration testing is conducted frequently to spot risks and manage them to attain higher security standards. The methodology of penetration checking includes 3 phases: test preparation, test and test analysis. The test phase involves the subsequent steps: data gathering, vulnerability analysis, and vulnerability exploit.

Introduction:

Security is one of the major problems of information systems. The growing property of computers through the web, the increasing extensibility of systems, and the uncurbed growth of the size and complexness of systems have created software system security a larger drawback currently than within the past. moreover, it is a business imperative to adequately defend an organization's info assets by following a comprehensive, and structured approach to produce protection from the risks an organization would possibly face. To solve the protection drawback and follow with the mandated security laws, security consultants have developed numerous security assurance methods including proof of correctness, layered design, software system engineering environments and penetration testing. Penetration testing could be a comprehensive technique to check the entire, integrated, operational, and trustworthy computing base that consists of hardware, software system and folks. The method involves an active analysis of the system for any potential vulnerabilities, including poor or improper system configuration, hardware and software system flaws, and operational weaknesses within the method or technical countermeasures

A security test helps to ensure the behaviour of the system security management, whereas a PEN test helps to determine the extent of issue for an attacker to penetrate an organization computing network. PEN test an unauthorized attack is demonstrated by a user on the test target system using automatic programmed tools, manual tools or both.

So, we decided to proceed further with the following Problem Statement:

Perform Penetration Testing for finding different possible vulnerabilities in web applications/apps/web services to prepare a finished report for the same. and eventually, do mapping and layer creation using the navigator tool.

This report is organized as follows:

In Section 2 - Related Work is described.

Section 3 contains our proposed idea.

Section 4 contains Methodology used.

Section 5 contains the Results obtained.

Section 6 contains Discussion and Future Work.

Section 7 contains the Conclusion of our work.

Related Work

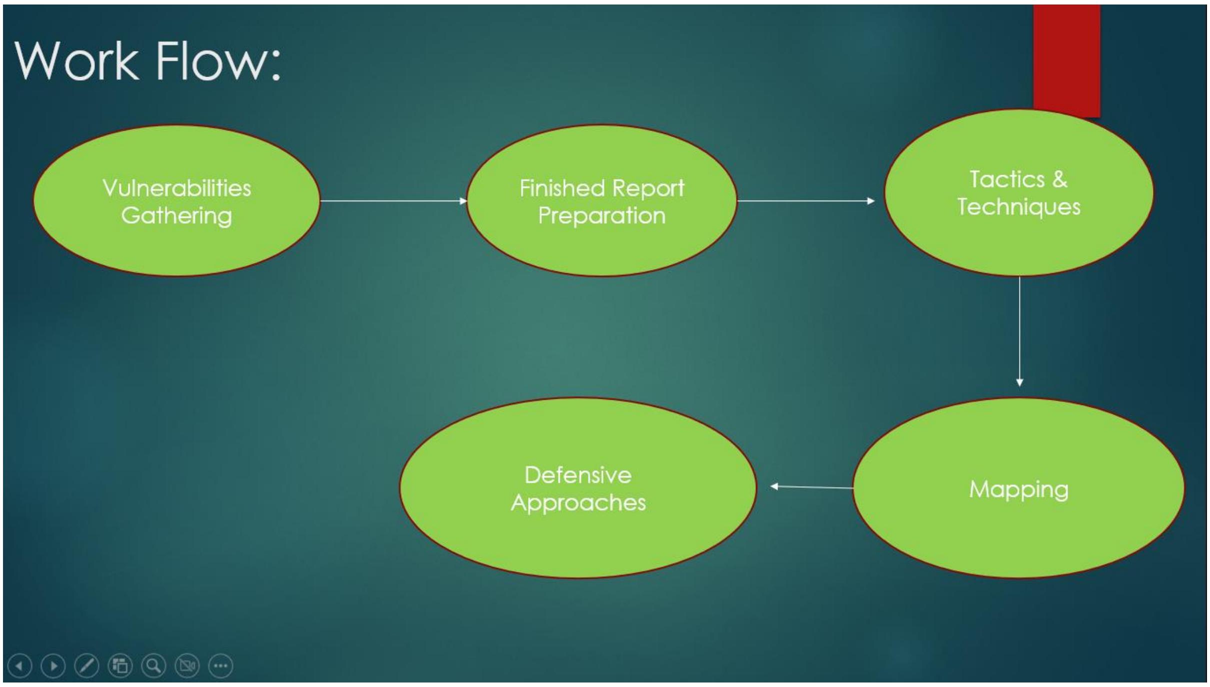
- The penetration testing process described by Neumann [1] includes four steps: The first step is to understand the system, the Second step is to generate a hypothesis about the flaws, the third step is testing to confirm or reject the hypotheses, and the last step is to extend the successful tests with additional hypotheses.
- Pfleeger [2] described an organized methodology for planning a suite of penetration tests that involves three steps: The first step is identifying vulnerable objects, the second step is determining the points of vulnerability of those objects, and the third is testing the vulnerability to determine the adequacy of controls.
- Botella [3] introduces a risk assessment-driven approach for performing and automating vulnerability testing of web applications called risk-based vulnerability testing. This approach is designed for security testing and adapts model-based testing techniques.
- Kals [4] presents a general web vulnerability scanner that automatically analyzes web pages to find exploitable SQL injection and XSS vulnerabilities. The authors also discuss the types of security tests, black box, and white box, related to the operation of the tool.

Proposed Idea:

To perform penetration testing to find various possible vulnerabilities in various web applications, apps, and web services to prepare a finished report for the same, and eventually, we will be performing mapping and layer creation using the navigator tool to detect the possible attacks along with the possible defensive approaches for the same. The main idea behind this proposal is to make an organisation aware of the possible attacks by analysing the vulnerabilities present and suggesting defensive approaches to make them secure.

Methodology:

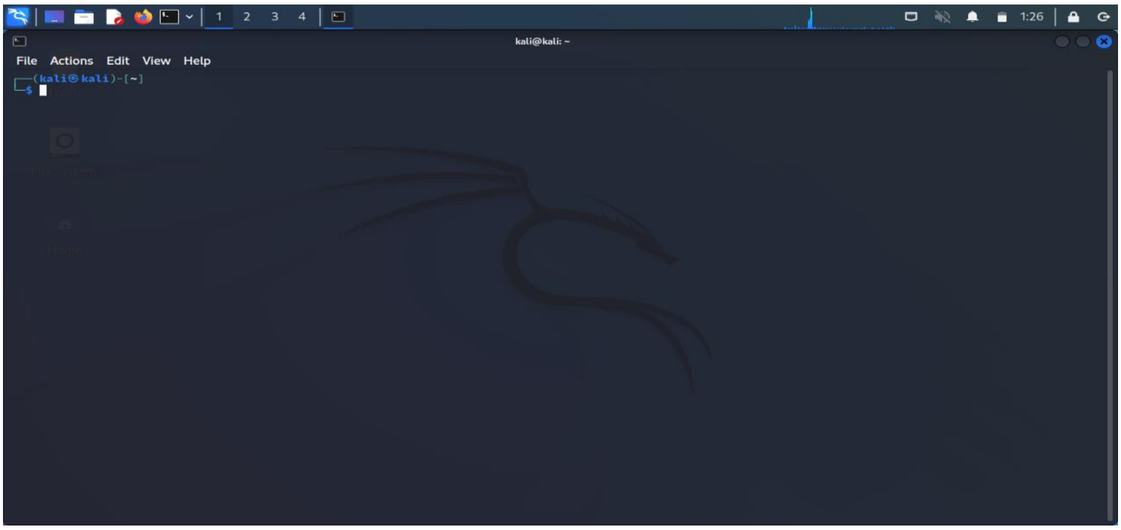
The workflow is shown below diagrammatically:



Work Flow:

To implement the above-mentioned proposed solution, the following steps are followed:

1. The virtual environment was initially set up for Kali Linux inside a VMware workstation, as shown in the below diagram.

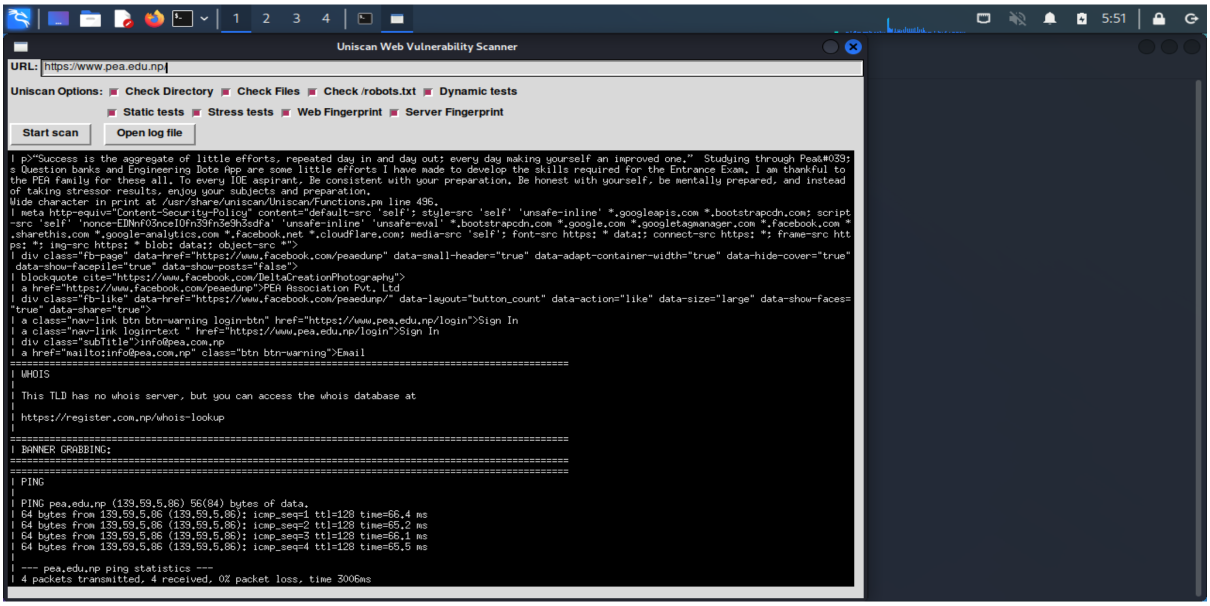


```
┌──(kali㉿kali)-[~]
└─$ 
```

Fig 1: Kali Linux Setup

2. The below mentioned tools were used to find different possible vulnerabilities in different web sites:

- Uniscan: Uniscan is the one to come back to when you need a quick-and-dirty web scanner that's noob-friendly which comes with the GUI and provides the report as a output. It was used to gather information about different web sites. One of them is https://www.pea.edu.np/. The collected information related to this web site using Uniscan is mentioned below:



URL: https://www.pea.edu.np/

Uniscan Options: ☒ Check Directory ☒ Check Files ☒ Check /robots.txt ☒ Dynamic tests
☒ Static tests ☒ Stress tests ☒ Web Fingerprint ☒ Server Fingerprint

```
| p>"Success is the aggregate of little efforts, repeated day in and day out; every day making yourself an improved one."  Studying through Pea&#039;
s Question banks and Engineering Dote App are some little efforts I have made to develop the skills required for the Entrance Exam. I am thankful to
the PEA family for these all. To every IOE aspirant, Be consistent with your preparation. Be honest with yourself, be mentally prepared, and instead
of taking stressor results, enjoy your subjects and preparation.
Wide character in print at /usr/share/uniscan/Uniscan/Functions.pm line 496.
| meta http-equiv="Content-Security-Policy" content="default-src 'self'; style-src 'self' 'unsafe-inline' *.googleapis.com *.bootstrapcdn.com; script
-src 'self' 'nonce-EDNnf03nceI0fn39fn3e9h3sdfa' 'unsafe-inline' 'unsafe-eval' *.bootstrapcdn.com *.google.com *.googletagmanager.com *.facebook.com *
.sharethis.com *.google-analytics.com *.facebook.net *.cloudflare.com; media-src 'self'; font-src https: * data:; connect-src https: *; frame-src htt
ps: *; img-src https: * blob: data:; object-src *">
| div class="fb-page" data-href="https://www.facebook.com/peaedunp" data-small-header="true" data-adapt-container-width="true" data-hide-cover="true"
 data-show-facepile="true" data-show-posts="false">
| blockquote cite="https://www.facebook.com/DeltaCreationPhotography">
| a href="https://www.facebook.com/peaedunp">PEA Association Pvt. Ltd
| div class="fb-like" data-href="https://www.facebook.com/peaedunp/" data-layout="button_count" data-action="like" data-size="large" data-show-faces=
"true" data-share="true">
| a class="nav-link btn btn-warning login-btn" href="https://www.pea.edu.np/login">Sign In
| a class="nav-link login-text " href="https://www.pea.edu.np/login">Sign In
| div class="subTitle">info@pea.com.np
| a href="mailto:info@pea.com.np" class="btn btn-warning">Email
====================================================================================================
| WHOIS
|
| This TLD has no whois server, but you can access the whois database at
|
| https://register.com.np/whois-lookup
|
====================================================================================================
| BANNER GRABBING:
====================================================================================================
====================================================================================================
| PING
|
| PING pea.edu.np (139.59.5.86) 56(84) bytes of data.
| 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=1 ttl=128 time=66.4 ms
| 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=2 ttl=128 time=65.2 ms
| 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=3 ttl=128 time=66.1 ms
| 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=4 ttl=128 time=65.5 ms
|
| --- pea.edu.np ping statistics ---
| 4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

Fig 2: Uni Scan Scanner

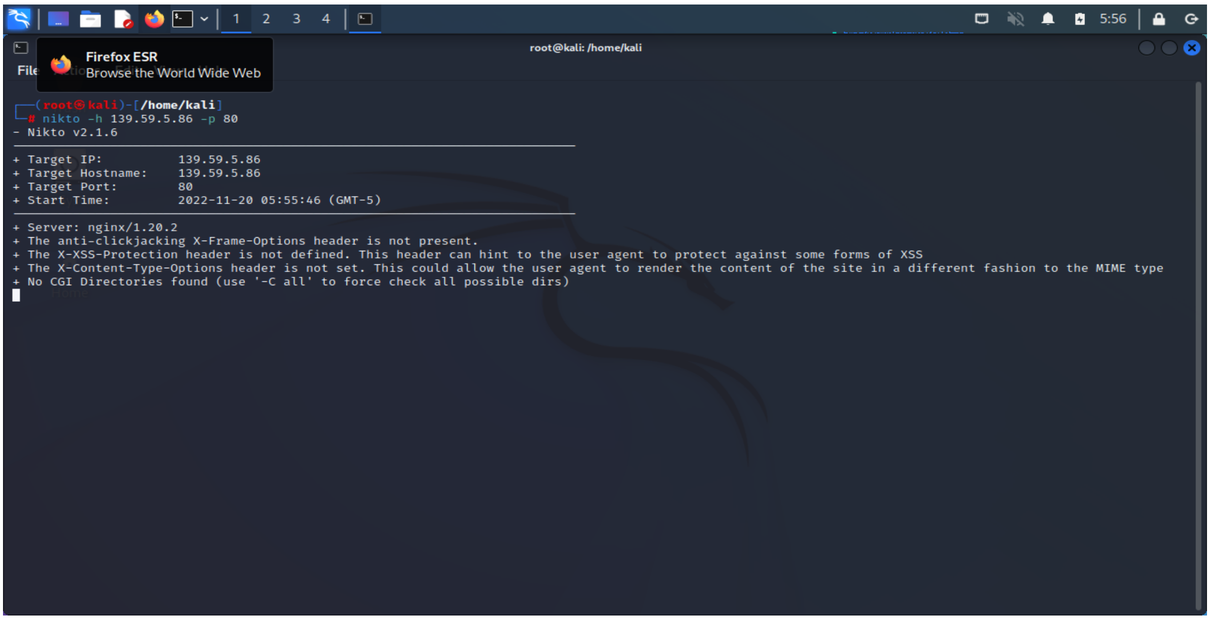
- **Scan date: 20-11-2022 1:37:38**
- ==
- **| Domain: https://www.pea.edu.np/**
- **| Server: nginx/1.20.2**
- **| IP: 139.59.5.86**
- ==
- ==
- **| Looking for Drupal plugins/modules**
- |
- ==
- **| WEB SERVICES**
- |
- ==
- **| FAVICON.ICO**
- |
- **| Web service Found (favicon.ico): Zero byte favicon**
- ==
- **| ERROR INFORMATION**
- |
- **| PEA Association Pvt. Ltd. Top and Best BE Entrance Preparation Center in Nepal GO TO HOMEPAGE**
- ==
- **| TYPE ERROR**
- |
- ==
- **| SERVER MOBILE**

- |
- ==
- | LANGUAGE
- |
- | lang="en"
- ==
- | INTERESTING STRINGS IN HTML
- |
- | !-- Payment methods -->
- | section class="payment-method">
- | div class="payment-wrapper">
- | div class="title">Our Payment Methods
- | div class="subTitle">You can pay for your courses conveniently with just a few clicks. We accept payments through online gateways such as E-Sewa and Khalti.
- | img src="https://www.pea.edu.np/assets/images/home/qbank.png" width="52" alt="PEA">
- | div class="icon-title">Question Bank
- | p>â€ œSuccess is the aggregate of little efforts, repeated day in and day out; every day making yourself an improved one.â€ • Studying through Pea&#039;s Question banks and Engineering Dote App are some little efforts I have made to develop the skills required for the Entrance Exam. I am thankful to the PEA family for these all. To every IOE aspirant, Be consistent with your preparation. Be honest with yourself, be mentally prepared, and instead of taking stressor results, enjoy your subjects and preparation.
- | meta http-equiv="Content-Security-Policy" content="default-src 'self'; style-src 'self' 'unsafe-inline' *.googleapis.com *.bootstrapcdn.com; script-src 'self' 'nonce-EDNnf03nceIOfn39fn3e9h3sdfa' 'unsafe-inline' 'unsafe-eval' *.bootstrapcdn.com *.google.com *.googletagmanager.com *.facebook.com *.sharethis.com *.google-analytics.com *.facebook.net *.cloudflare.com; media-src 'self'; font-src https: * data:; connect-src https: *; frame-src https: *; img-src https: * blob: data:; object-src *">
- | div class="fb-page" data-href="https://www.facebook.com/peaedunp" data-small-header="true" data-adapt-container-width="true" data-hide-cover="true" data-show-facepile="true" data-show-posts="false">
- | blockquote cite="https://www.facebook.com/DeltaCreationPhotography">
- | a href="https://www.facebook.com/peaedunp">PEA Association Pvt. Ltd
- | div class="fb-like" data-href="https://www.facebook.com/peaedunp/" data-layout="button_count" data-action="like" data-size="large" data-show-faces="true" data-share="true">
- | a class="nav-link btn btn-warning login-btn" href="https://www.pea.edu.np/login">Sign In
- | a class="nav-link login-text " href="https://www.pea.edu.np/login">Sign In
- | div class="subTitle">info@pea.com.np
- | a href="mailto:info@pea.com.np" class="btn btn-warning">Email
- ==
- | WHOIS
- |
- | This TLD has no whois server, but you can access the whois database at
- |
- | https://register.com.np/whois-lookup
- |
- ==
- | BANNER GRABBING:
- ==
- ==
- | PING
- |
- | PING pea.edu.np (139.59.5.86) 56(84) bytes of data.
- | 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=1 ttl=128 time=63.5 ms
- | 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=2 ttl=128 time=67.1 ms
- | 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=3 ttl=128 time=64.8 ms

```
| 64 bytes from 139.59.5.86 (139.59.5.86): icmp_seq=4 ttl=128 time=65.1 ms
|
| --- pea.edu.np ping statistics ---
| 4 packets transmitted, 4 received, 0% packet loss, time 3022ms
| rtt min/avg/max/mdev = 63.481/65.107/67.084/1.289 ms
==============================================================================================
| TRACEROUTE
|
| traceroute to www.pea.edu.np (139.59.5.86), 30 hops max, 60 byte packets
|  1  192.168.179.2 (192.168.179.2)  0.140 ms  0.093 ms  0.082 ms
|  2  * * *
|  3  * * *
|  4  * * *
|  5  * * *
|  6  * * *
|  7  * * *
|  8  * * *
|  9  * * *
| 10  * * *
| 11  * * *
| 12  * * *
| 13  * * *
| 14  * * *
| 15  * * *
| 16  * * *
| 17  * * *
| 18  * * *
| 19  * * *
| 20  * * *
| 21  * * *
| 22  * * *
| 23  * * *
| 24  * * *
| 25  * * *
| 26  * * *
| 27  * * *
| 28  * * *
| 29  * * *
| 30  * * *
==============================================================================================
| NSLOOKUP
|
| Server:         192.168.179.2
| Address: 192.168.179.2#53
|
| Non-authoritative answer:
| www.pea.edu.np  canonical name = pea.edu.np.
| pea.edu.np      mail exchanger = 50 mx3.zoho.com.
| pea.edu.np      mail exchanger = 20 mx2.zoho.com.
| pea.edu.np      mail exchanger = 10 mx.zoho.com.
| Authoritative answers can be found from:
| pea.edu.np      nameserver = ns2.digitalocean.com.
| pea.edu.np      nameserver = ns1.digitalocean.com.
| ns2.digitalocean.com            internet address = 173.245.59.41
| ns1.digitalocean.com        internet address = 173.245.58.51
| ns2.digitalocean.com        has AAAA address 2400:cb00:2049:1::adf5:3b29
| ns1.digitalocean.com        has AAAA address 2400:cb00:2049:1::adf5:3a33
| pea.edu.np
|         origin = ns1.digitalocean.com
|         mail addr = hostmaster.pea.edu.np
|         serial = 1612665825
|         refresh = 10800
|         retry = 3600
|         expire = 604800
|         minimum = 1800
| Name:   pea.edu.np
| Address: 139.59.5.86
| pea.edu.np      text = "zoho-verification=zb00357588.zmverify.zoho.com"
| pea.edu.np      text = "v=spf1 include:zoho.com ~all"
===========================================================================================
| NMAP
|
| Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-20 01:38 EST
| NSE: Loaded 155 scripts for scanning.
| NSE: Script Pre-scanning.
| Initiating NSE at 01:38
| Completed NSE at 01:38, 0.00s elapsed
| Initiating NSE at 01:38
| Completed NSE at 01:38, 0.00s elapsed
| Initiating NSE at 01:38
| Completed NSE at 01:38, 0.00s elapsed
| Initiating Ping Scan at 01:38
| Scanning www.pea.edu.np (139.59.5.86) [4 ports]
| Completed Ping Scan at 01:38, 0.04s elapsed (1 total hosts)
| Initiating Parallel DNS resolution of 1 host. at 01:38
| Completed Parallel DNS resolution of 1 host. at 01:38, 0.00s elapsed
| Initiating SYN Stealth Scan at 01:38
| Scanning www.pea.edu.np (139.59.5.86) [1000 ports]
| Discovered open port 443/tcp on 139.59.5.86
| Discovered open port 80/tcp on 139.59.5.86
| Discovered open port 22/tcp on 139.59.5.86
| Completed SYN Stealth Scan at 01:38, 5.39s elapsed (1000 total ports)
| Initiating Service scan at 01:38
| Scanning 3 services on www.pea.edu.np (139.59.5.86)
| Completed Service scan at 01:38, 5.01s elapsed (3 services on 1 host)
| Initiating OS detection (try #1) against www.pea.edu.np (139.59.5.86)
| Initiating Traceroute at 01:38
| Completed Traceroute at 01:38, 9.09s elapsed
| NSE: Script scanning 139.59.5.86.
| Initiating NSE at 01:38
| Completed NSE at 01:39, 27.87s elapsed
| Initiating NSE at 01:39
| Completed NSE at 01:39, 2.71s elapsed
| Initiating NSE at 01:39
| Completed NSE at 01:39, 0.01s elapsed
| Nmap scan report for www.pea.edu.np (139.59.5.86)
| Host is up (0.014s latency).
| Not shown: 997 filtered tcp ports (no-response)
| PORT    STATE SERVICE    VERSION
| 22/tcp  open  tcpwrapped
| |_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
| 80/tcp  open  tcpwrapped
| | http-methods:
| |_  Supported Methods: OPTIONS
| |_http-title: Did not follow redirect to https://www.pea.edu.np/
| 443/tcp open  tcpwrapped
| |_http-favicon: Unknown favicon MD5: FE5B4F1027C80172D2189203874E61F9
| |_ssl-date: TLS randomness does not represent time
| | http-methods:
| |_  Supported Methods: HEAD OPTIONS
| |_http-server-header: nginx/1.20.2
| | ssl-cert: Subject: commonName=pea.edu.np
| | Subject Alternative Name: DNS:pea.edu.np, DNS:www.pea.edu.np
| | Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| | Public Key type: rsa
| | Public Key bits: 2048
| | Signature Algorithm: sha256WithRSAEncryption
| | Not valid before: 2022-10-27T02:29:51
| | Not valid after:  2023-01-25T02:29:50
| | MD5:   06e491380c1d934d004bbf9250d02757
| |_SHA-1: 6fc8b547b821b5317780264f72873251d0246185
| Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
| Device type: WAP|phone
| Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
| OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
| OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
|
| TRACEROUTE (using port 80/tcp)
| HOP RTT    ADDRESS
| 1   ... 30
|
| NSE: Script Post-scanning.
| Initiating NSE at 01:39
| Completed NSE at 01:39, 0.00s elapsed
| Initiating NSE at 01:39
| Completed NSE at 01:39, 0.00s elapsed
| Initiating NSE at 01:39
| Completed NSE at 01:39, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
| OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
| Nmap done: 1 IP address (1 host up) scanned in 55.27 seconds
|           Raw packets sent: 2169 (98.044KB) | Rcvd: 7 (292B)
==============================================================================================
========
|
| Directory check:
| [+] CODE: 200 URL: https://www.pea.edu.np/blogs/
| [+] CODE: 200 URL: https://www.pea.edu.np/news/
```

- Nikto: Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over

6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. This tool was also used to gather information related to different web sites. One of them is https://www.pea.edu.np/. The collected information related to this web site using Nikto is mentioned below:



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h 139.59.5.86 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          139.59.5.86
+ Target Hostname:    139.59.5.86
+ Target Port:        80
+ Start Time:         2022-11-20 05:55:46 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.20.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Fig 3: Nikto Scanner

```
┌──(root㉿kali)-[/home/kali]

└─# nikto -h 139.59.5.86 -p 80

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP:        139.59.5.86

+ Target Hostname:    139.59.5.86

+ Target Port:        80

+ Start Time:        2022-11-20 02:21:44 (GMT-5)
```

+ Server: nginx/1.20.2

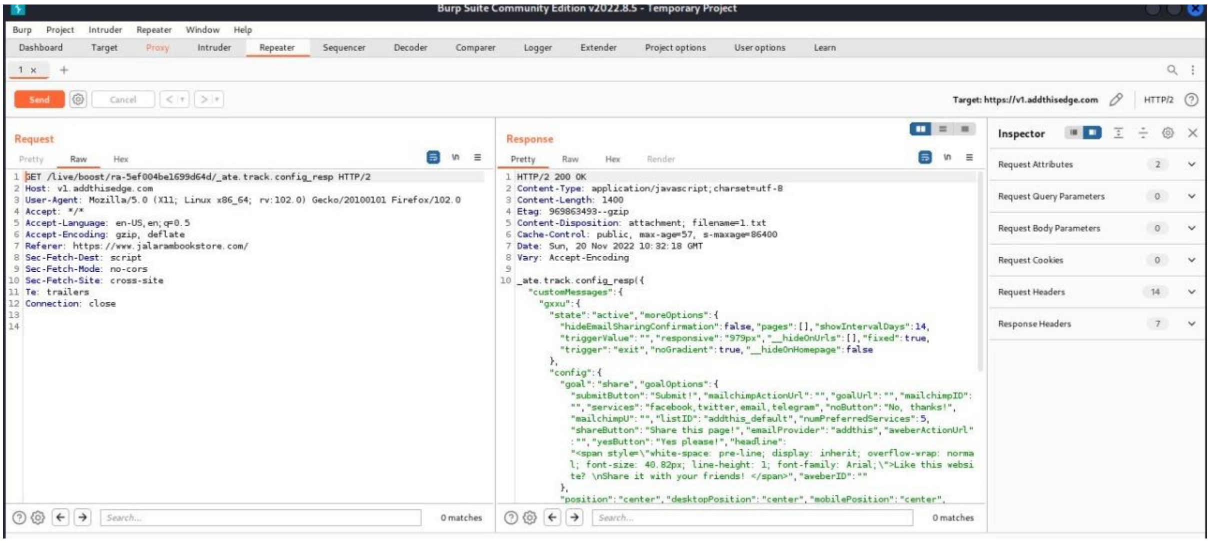
+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

- Burp suite: Burp or Burp Suite is a set of tools used for penetration testing of web applications. Burp Suite aims to be an all-in-one set of tools like: Spider, proxy etc. The operations performed using burp suite has been demonstrated in the attached demo video. Using this tool, cross site scripting attack has been performed which is also there in the attached demo video.


Burp Suite Community Edition v2022.8.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 0
Request Headers 14
Response Headers 7
Search... 0 matches

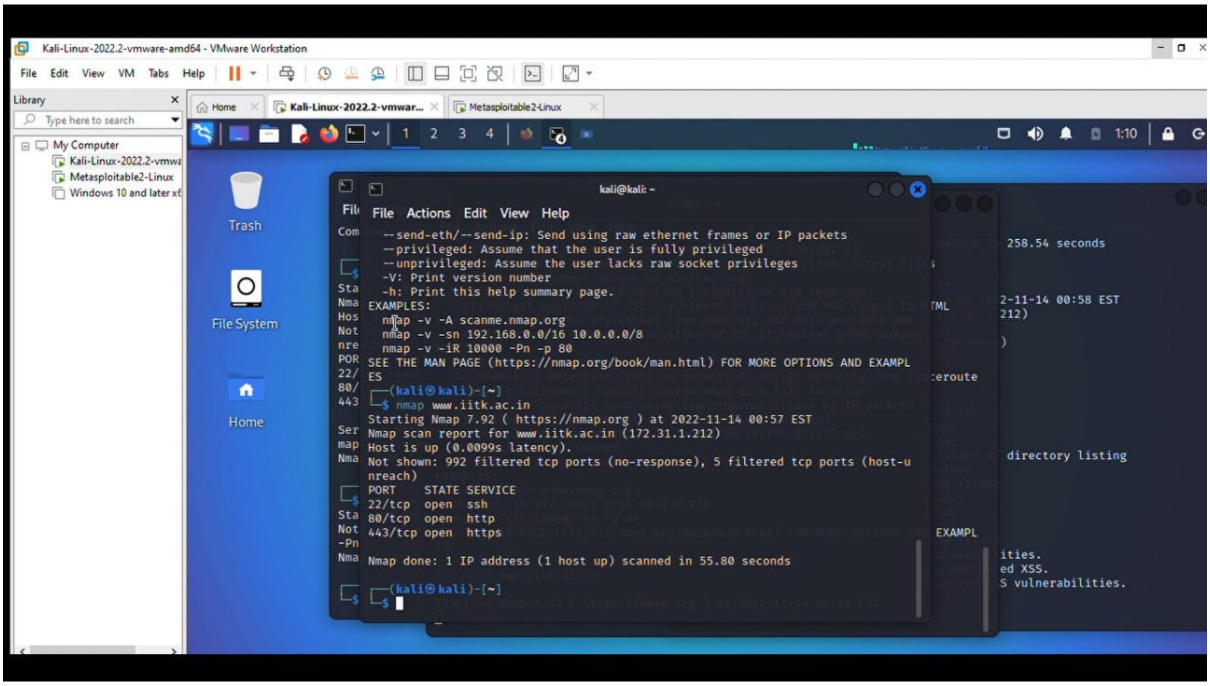
Target: https://v1.addthisedge.com

```
GET /live/boost/ra-5ef004be1699d64d/_ate.track.config_resp HTTP/2
Host: v1.addthisedge.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.jalarambookstore.com/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close


```

```
HTTP/2 200 OK
Content-Type: application/javascript;charset=utf-8
Content-Length: 1400
Etag: 969863493--gzip
Content-Disposition: attachment; filename=1.txt
Cache-Control: public, max-age=57, s-maxage=86400
Date: Sun, 20 Nov 2022 10:32:18 GMT
Vary: Accept-Encoding

_ate.track.config_resp({
  "customMessages":{
    "gxxu":{
      "state":"active","moreOptions":{
        "hideEmailSharingConfirmation":false,"pages":[],"showIntervalDays":14,
        "triggerValue":"","responsive":"979px","__hideOnUrls":[],"fixed":true,
        "trigger":"exit","noGradient":true,"__hideOnHomepage":false
      },
      "config":{
        "goal":"share","goalOptions":{
          "submitButton":"Submit!","mailchimpActionUrl":"","goalUrl":"","mailchimpID":
          "","services":"facebook,twitter,email,telegram","noButton":"No, thanks!",
          "mailchimpU":"","listID":"addthis_default","numPreferredServices":5,
          "shareButton":"Share this page!","emailProvider":"addthis","aweberActionUrl"
          :"","yesButton":"Yes please!","headline":
          "<span style=\"white-space: pre-line; display: inherit; overflow-wrap: norma
          l; font-size: 40.82px; line-height: 1; font-family: Arial;\">Like this websi
          te? \nShare it with your friends! </span>","aweberID":""
        },
        "position":"center","desktopPosition":"center","mobilePosition":"center",
```

<u>Fig 4: Burp Suite</u>

- Nmap: Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. The operations performed using Nmap has been demonstrated in the attached demo video.



```
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES
┌──(kali㉿kali)-[~]
└─$ nmap www.iitk.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-14 00:57 EST
Nmap scan report for www.iitk.ac.in (172.31.1.212)
Host is up (0.0099s latency).
Not shown: 992 filtered tcp ports (no-response), 5 filtered tcp ports (host-u
nreach)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 55.80 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 5: Nmap

3. By observing the gathered information from the tools, some of the below-mentioned related attacks were performed successfully for the respective vulnerabilities which have been demonstrated in the attached video.

    - Cross site scripting attack
    - D-Dos attack

4. The finished report was prepared based on the following criteria: In the case where we were able to perform the attack, we prepared the finished report after the attack was done.

On the other hand, with the help of the list of vulnerabilities provided by the tool, we gathered the different possible procedures of attack for the same and then prepared the finished report.

The prepared finished report has been illustrated below as per the information gathered using different penetration testing tools in different web sites and with the help of performed attacks and the below mentioned finished report has been termed as “Surakcha Attack Finished Report:

In this report, we have described our findings in detail, including technical analysis of the gathered information related to different vulnerabilities along with their approaches.

Nikto detected a missing X-Frame-Options header. The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. The tested site lacks the X-XSS-Protection header. This header hints to the user agent to protect against some forms of XSS. The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute.

The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user’s machine under the guise of the vulnerable site. The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.

The server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack and the XSS attack has been performed using burpsuite in the proposed solution and has been demonstrated in the attached demo video. Numerous incidents have demonstrated that open ports are most vulnerable to attack when the services listening to them are unpatched or insufficiently protected or misconfigured, which can lead to

compromised systems and networks. In these cases, threat actors can use open ports to perform various cyberattacks that exploit the lack of authentication mechanisms in the TCP and UDP protocols. One common example is spoofing, where a malicious actor impersonates a system or a service and sends malicious packets, often in combination with IP spoofing and man-in-the-middle-attacks. The campaign against RDP Pipe Plumbing is one of the latest to employ such a tactic. In addition, ports that have been opened on purpose (for instance, on a web server) can be attacked via that port using application-layer attacks such as SQL injection, cross-site request forgery and directory traversal.

Another common technique is the denial of service (DoS) attack, most frequently used in the form of distributed denial of service (DDoS) which has been performed in the proposed solution within the virtual environment between two virtual machines and has been demonstrated in the attached demo video, where attackers send massive numbers of connection requests from various machine to the service on the target to deplete its resources.

Any port can be targeted by threat actors, but some are more likely to fall prey to cyberattacks because they commonly have serious shortcomings, such as application vulnerabilities, lack of two-factor authentication and weak credentials. Many open ports were detected by nmap while performing the penetration testing.

Here are the most vulnerable ports regularly used in attacks:

Ports 20 and 21 (FTP)

Port 20 and (mainly) port 21 are File Transfer Protocol (FTP) ports that let users send and receive files from servers. FTP is known for being outdated and insecure. As such, attackers frequently exploit it through:

- ***Brute-forcing passwords***
- ***Anonymous authentication (it's possible to log into the FTP port with "anonymous" as the username and password)***
- ***Cross-site scripting***
- ***Directory traversal attacks***

Port 22 (SSH)

Port 22 is for Secure Shell (SSH). It's a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.

Port 23 (Telnet)

Port 23 is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it's still used by some websites. Since it's outdated and insecure, it's vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.

Port 25 (SMTP)

Port 25 is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming.

Port 53 (DNS)

Port 53 is for Domain Name System (DNS). It's a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks.

Ports 137 and 139 (NetBIOS over TCP) and 445 (SMB)

Server Message Block (SMB) uses port 445 directly and ports 137 and 139 indirectly. Cybercriminals can exploit these ports through:

- ***Using the Eternal Blue exploit, which takes advantage of SMBv1 vulnerabilities in older versions of Microsoft computers (hackers used Eternal Blue on the SMB port to spread WannaCry ransomware in 2017)***
- ***Capturing NTLM hashes***
- ***Brute-forcing SMB login credentials***

Ports 80, 443, 8080 and 8443 (HTTP and HTTPS)

HTTP and HTTPS are the hottest protocols on the internet, so they're often targeted by attackers. They're especially vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

Ports 1433,1434 and 3306 (Used by Databases)

These are the default ports for SQL Server and MySQL. They are used to distribute malware or are directly attacked in DDoS scenarios. Quite often, attackers probe these ports to find unprotected database with exploitable default configurations.

Port 3389 (Remote Desktop)

This port is used in conjunction with various vulnerabilities in remote desktop protocols and to probe for leaked or weak user authentication. Remote desktop vulnerabilities are currently the most-used attack type; one example is the Blue Keep vulnerability.

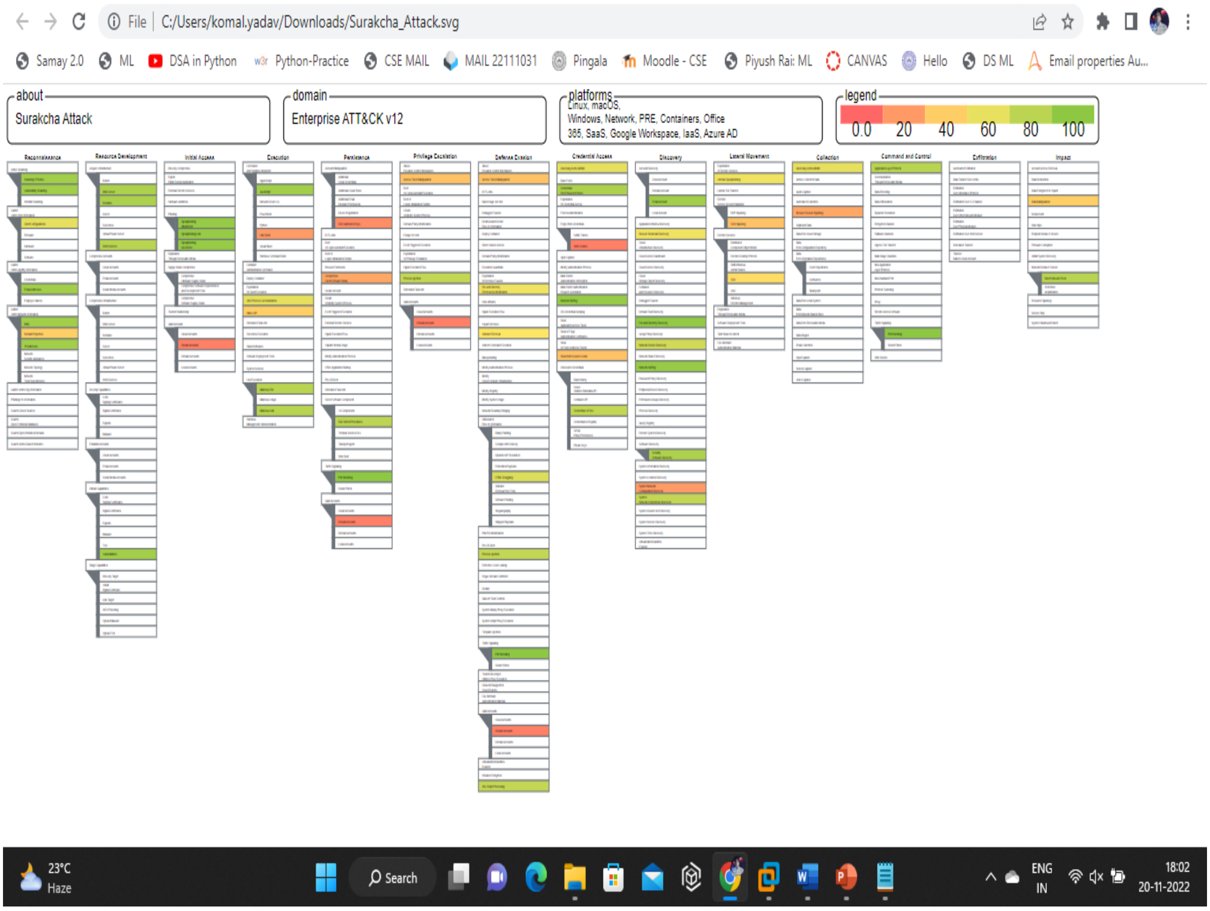
The below listed are the vulnerabilities gathered by the uniscan tool;

- ***Local file include(LFI)***
- ***Remote command execution(RCE)***
- ***Remote file include(RFI) • Cross-site scripting(XSS)***
- ***Sql and blind sql injection***

Following are the lists of Vulnerabilities scanned by nikto scanner

- ***Server and software miss configuration***
- ***Default files and programs***
- ***Insecure files and programs***
- ***Outdated servers and programs.***

5. With the help of a finished report, we found out the related tactics and techniques, and then, with the help of the ATT&CK navigator tool, we created a layer and performed a mapping of the discovered techniques under a specific tactic. The done mapping has been illustrated below diagrammatically.



File | C:/Users/komal.yadav/Downloads/Surakcha_Attack.svg

about: Surakcha Attack

domain: Enterprise ATT&CK v12

platforms: Linux, macOS, Windows, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD

legend: 0.0 20 40 60 80 100

Fig 6: Mapping using ATT&CK Navigator Tool

6. Eventually, a list of defensive approaches was prepared after performing a mapping using the Navigator tool which are illustrated below:

   ➢ Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

   - X-Frame-Options: DENY It completely denies being loaded in frame/iframe.

   - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.

- X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in an iframe. However please pay attention to that, not all browsers support this.

- Employing defensive code in the UI to ensure that the current frame is the most top-level window.

- Set the X-XSS-Protection header
- Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'.
- Patch firewalls regularly.
- Check ports regularly.
- Use IDP and IPS tools.
- Use SSH Keys.
- Conduct penetration tests and vulnerability assessments.

Discussion and Future work

As per our project, we had done some penetration testing and find the vulnerability in different websites. But penetration testing has no limit. Penetration testing is more about practice and experience. Here some future work that can also be done to provide more efficient and suitable penetration testing –

In future, AI and ML can help in penetration testing.

Basically, penetration testing has different phases –

- Information Gathering: In this phase, a pen tester tries to gather as much information as possible about the target. So, AI and ML can help the pen tester to gather the information automatically about the target.

- Vulnerability Assessment: In this phase, pen tester tries to detect different vulnerability. So, AI and ML can help the pen tester to find different types of vulnerability in any web applications using collected or gathered information and can remove that is not applicable.

- Exploitation: In this phase, pen tester put action based on his plans for example: gain access, data exfiltration, lateral movement etc. So, AI and ML can help to perform this action automatically based on above information.

In future, using of AI and ML cam make penetration testing more accurate and evaluation more efficient. But it is also important that penetration testing requires more practice and experience to decide best course of action.

Conclusion:

The above proposed solution plays a great role in preventing an organisation from different possible attacks with the help of gathered information and vulnerabilities using different penetration testing tools. By analysing different collected information related to a particular website and a prepared finished report, one can easily find the possible techniques under a particular tactic that can be used for an attack. Also, by analysing the done mapping using ATT&CK navigator tool, an organisation can be aware of different possible threat groups which can perform the attack by comparing the similarity between the prepared mapping with the default mapping of different threat groups. This paper addressed various tools opted for scanning web vulnerabilities and the possible attacks. We identified that what vulnerabilities a specific tool is efficient to detect by running various web applications on each tool. Uniscan tool has many significant features including within it that are not present in other tools i.e., nikto, The vulnerabilities such as file insertion attack, local file include and blind SQL injection are not present in other tools. Burp suite consists of many other sub tools that can be used in a house together to gather the information and the Nmap is the best tool to fetch out the network and Ip addresses related information. This approach of keeping an organisation secure can be enhanced further with the implementation of AI and ML as discussed in the discussion and future work section.

References

[1]

[1] Neumann, P. (1977) “Computer System Security Evaluation,” Proceedings of AFIPS 1977 Natl. Computer Conf., Vol. 46, pp. 1087-1095.

[2] Pfleeger, C. P., Pfleeger, S. L., and Theofanos, M. F. (1989) “A Methodology for Penetration Testing,” Computers &Security, 8(1989) pp. 613-620.

[3] Botella J, Legeard B, Peureux F, Vernotte A (2014) Risk-based vulnerability testing using security test patterns(Margaria T, Steffen B, eds.). Springer, Berlin.

[4] Kals S, Kirda E, Kruegel C, Jovanovic N (2006) Secubat: a web vulnerability scanner In: Proceedings of the 15th International Conference on World Wide Web. WWW ’06, 247–256.. ACM, New York,.

[5] https://mitre-attack.github.io/attack-navigator/

[6] https://nmap.org/

[7] https://cirt.net/Nikto2

[8] https://www.geeksforgeeks.org/what-is-burp-suite/

[9] https://www.geeksforgeeks.org/uniscan-web-application-penetration-testing-tool/

[10] https://www.kali.org/

[11] https://ermprotect.com/blog/how-artificial-intelligence-will-drive-the-future-of-penetration- testing/