Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

Analysis of Different Methods of Reconnaissance

Pavan Kashyap[1,*], Vinesha Selvarajah [2]

[1,2] *Asia Pacific University of Technology & Innovation, Malaysia*
[*] *Corresponding author. Email: tp056083@mail.apu.edu.my*

ABSTRACT
In the current digital world, we are exposed to a host of information. There's an immense wealth of knowledge base which can be tapped. While this could be used in good ways, there are possibilities of misuse of this information, for example, these days hacking websites is a common occurrence and this can compromise the security of the website, leading sometimes to consequences that can be even serious. In this article, the focus is on one of the important phases known as "reconnaissance", which is step one in the methods of website hacking. This article uses the "Passive" method of gathering information. Different "OSINT" tools involved in the information gathering are used and the comparison of their performances is made against certain pre-determined outcomes. These various tools are used on two different websites one secure and another one vulnerable to ascertain variable outcomes depending on the level of security of each type of website. Various information is gathered by using the different tools which would be essential to perform the other steps followed after reconnaissance in the website hacking. An extensive analysis is also conducted to understand the consequences of website hacking on a company in the current scenario.

Keywords: *OSINT tools, Reconnaissance, Website hacking, Website security.*

1. INTRODUCTION

In today's world digitalization as we call it is present in all aspects of our daily lives in all possible ways. The impact of digitalization is prevalent in every spectrum of our lives and the current era is known as the "digital era". Right from gathering news and performing phone to other various activities can be performed with the help of technology. The use of technology has showcased a significant evolution over the past 2 decades. This has made people's life easier as well as connected multiple people from different parts of the world with the touch of a button [1]

In today's world, almost all organizations from different sectors have transformed their way of providing services. It can be inferred that every entity has moved into the internet and left its mark. Every company is it small or large nowadays is present with their website which provides a lot of information regarding the employees, location of the company, the services provided and many more details. As more and more people are present on the internet there has been an upward trajectory in the number of cybercrimes. Cybercrime is also known as computer crime makes use of the computer as an instrument to commit fraud such as stealing identity, trafficking in child pornography, violating the privacy, and many others [2]. Therefore, it can be understood that the security of the users is in danger when they perform the activity on the internet world. One of the main threats for companies on the web is website security.

There are many multiple phases involved in the process of performing website hacking. The steps should be performed in an orderly manner as follows:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing tracks

The main goal of this article will be solely based on "Reconnaissance". The purpose of Reconnaissance is to gather information. Information gathering and getting to know more about the target system is the first process that is involved in ethical hacking. This step is done to gain details regarding the target machine which could help provide multiple information such as confidential details, network details, security vulnerabilities IP location, and many more. There are mainly two types of Reconnaissance that could be performed which are known as "active" and "passive" [3]. This article will focus on both the passive method and the active method of gathering information. Passive reconnaissance is a method through which attempts are made to gather

information about the target and its network without actively being involved with the system. Active reconnaissance is a method in which attempts are made to gather information through actively engaging with the system. With the advancements that have taken there has been an increase in the usage of the internet nowadays due to which passive method has also become common and is being performed by many people [4].

2. MATERIALS AND METHODS

There are many tools such as Shodan.io, Wireshark, Wappalyzer, and many more are discussed in greater detail on how it works, and the demonstration of these tools is also performed on 2 different websites one Secure and another one vulnerable. There has been an analysis done on the tools and their properties.

2.1. Wireshark

Wireshark is an open-source reconnaissance tool used to perform network packet analysis. A network packet analyzer is also known as a “packet sniffer” showcases the captured data in as detail as possible. A packet analyzer is a piece of hardware or software used to monitor network traffic. The analyzer examines the data packets that pass between the computers on a network as well as between networked computers and the internet. There are 2 modes of capturing the data known as the “unfiltered” mode in this all the possible packets of data are captured while in the "filtered" mode analyzer will only capture packets that contain specific data elements. Packet sniffers can be used on both wired and wireless networks. A sniffer can record any data transmitted send it to a command-and-control server for further analysis. The efficiency of the sniffer depends on the security protocols implemented as this determines the amount of data that could be gathered [5] Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. However, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic.

There are multiple features present in Wireshark which makes it one of the most popular network analyzer tools. Firstly, it is a free tool that can be used on almost all different types of operating systems such as Linux, Windows, OS X, FreeBSD, NetBSD, etc. One of the other important features is that it is a three-pane packet browser while each browser providing different information. The first pane known as the packet list pane showcases a summary of each packet captured. By navigating on packets in this pane the user can control what is displayed in the other two panes. The second pane known as the packet details pane displays the packet selected in the packet list pane in more detail. The third pane known as the packet bytes pane displays the data from the packet selected in the packet list pane and highlights the field selected in the packet details pane [6]. Through the help of this tool more than hundreds of protocols can be analyzed and results will be provided which might be important for performing further investigations. Wireshark also supports a variety of well-documented capture file formats such as “PcapNg” and “Libpcap” these formats are used for storing the captured data therefore these features make this tool one of the most common and well-known tools among all ethical hackers.

2.2. Shodan.IO

Shodan.io is a search engine that is specifically designed for IoT devices. Shodan is a useful tool at the initial stage of testing. Moreover, allows intruders to quickly check how a given organization looks like as far as the Internet is concerned. It identifies the undetectable parts of the Internet most people will not ever see. Any connected device can show up in a search, such as servers, printers, webcams, traffic lights, Security cameras, Control systems. The engine immediately looks for systems that match your query in terms of vulnerability, affiliation with a given organization, the type of protocol used, location, and many other criteria. All of this can be performed without sending even a single ping towards the target system. Shodan can help penetration Testers to find valuable information about the target or all internet ports can help companies identify and prevent security vulnerabilities [7].

Few basic algorithms are followed by Shodan these are short and sweet. In other words, the algorithms can also be referred to as the functions which are performed by Shodan.

1. Generate a random IPv4 address. This means the tool provides different Ip addresses to the device or the system every single time. The IP address is a unique number that is assigned to each device or system present in the network. This IP address is an element that provides identity to any device or system present in the network.
2. Creates a random port to test from the list of ports that Shodan comprehends. This means the tool will every single time test to open different ports. These ports show some of the protocols that are running in the background of the system. These open ports might be vulnerable to attacks therefore it is helpful for intruders trying to gain information.
3. Check the random IPv4 address on the random port and grab a banner. Banner grabbing is a type of attack during which the attackers send requests to the system they are attempting to attack to gather more information about it. If the system is not well configured, it may leak information, such as the server version, PHP/ASP.NET version, OpenSSH version, etc., therefore this is one of the essential features provided by Shodan [8].

2.3. Nessus

A scanner that can be used on multiple Operating systems. Mistakes happen, even in the process of building and coding technology. What is left behind from these mistakes is commonly referred to as a bug. Many of these bugs can be taken advantage of by nefarious actors these are known as vulnerabilities. Vulnerabilities can be leveraged to force the software to act in ways it is not intended to, such as gleaning information about the current security defences in place. Therefore, in simple terms vulnerabilities can be understood as the threats that are present in any device or a system. Nessus is a remote security scanning tool that scans your computer and alerts you when it finds vulnerabilities that malicious hackers can use to access any computer that you have connected to the network. To do this, it performs more than 1,200 checks on a given computer, testing whether any of these attacks can be used to break into the computer or otherwise damage it. [9].

Nessus allows users to run an administrative console that performs a vulnerability scan and saves the database on a machine other than the server. Nessus provides plug-ins that are very similar to virus signatures and scan for common infected applications.

These plug-in programs are typically written in the NASL language (Nessus Attack Scripting Language) but they can be written in most languages. Plug-in updates need to be done frequently so the program has up-to-date vulnerability detection. The administrator using Nessus can either customize the scan or use the default scans, which are usually the preferred method for time-saving purposes. Users can also configure different levels of port scanning to consider firewalls and intrusion detection systems. For more accurate and detailed information about Windows-based hosts in a Windows domain, it is recommended that you create a domain group and an account with remote registry access. The format of the scan results is based on the domain, host, and related vulnerabilities. Reported weaknesses come with a multitude of suggestions, explaining the nature of the problem, and listing fixes [10].

2.4. Comparison of the tools

2.4.1. Wireshark VS TCPdump

S.No	Property	TCPdump	Wireshark
1	Os supported	Unix based	Windos and unix based
2	Disk usage	448kb	81mb (windows) & 449mb (unix)
3	Cost	Free	Free
4	Open source	yes	Yes
5	No. of protocols supported	Tep/ip	More than 1000
6	Libcap based	yes*	Yes
7	Multiple interface at a single instance	No	No
8	Alarms on traffic, pratocols	No	No
9	Decode protocol (Hex, ASCII EBCDIC)	Only hex and ASCII	Only hex and ACSII
10	Identify abnormal protocol	No	No (only creates a warning)
11	Identtify packets with forged data	No	Yes
12	Display protocol in OSI 7 layer structure	No	Yes
13	Locate hosts running a specific service	No	Yes
14	Network communication in matrix map	No	No
15	Evaluate critical business traffic and non-business traffic	Yes (by filter)	Yes (by creating filters)
16	Reconstruct TCP communication	No (by TCP flow)	Yes (but not formated)
17	UDP traffic	No	Yes

Figure 1 Comparison table of Wireshark Vs TCPdump [11]

Similarities

Both TCPdump and Wireshark have extensive packet filters to filter incoming traffic through the NIC. Neither TCPdump nor Wireshark has an intrusion detection feature. When passive attacks or anything strange happens on the network, they cannot generate attack alerts or warnings. If someone wants to manipulate data on the network, then they shouldn't be able to manipulate both tools. None of them can send the message in the network or do active things. Both tools capture files in libpcap format. Both can act as a command-line tool [11].

Differences

Wireshark has an easy-to-use interface that can display the information in the packet in an orderly manner. In contrast, TCPdump has no graphical interface. The graphical interface helps to understand the tool and work better. Compared with Wireshark, TCPdump and its filtering rules are more difficult to learn because the TCPdump rules seem completely mysterious at first. Wireshark helps to analyze the captured data packets and compare graphs with the limitations of the protocol, target IP, etc.

However, in TCPdump, if you do not use third-party tools, you cannot draw a single graph. Users only get information in the form of text words. In addition, the tool is more graphical, so system requirements increase. Therefore, compared with other methods, TCPdump has

the least overhead. In addition, TCPdump is the only tool that can be used remotely among the above tools because it has the least load on the system. TCPdump is also less invasive than Wireshark [11].

Overall based on the research conducted it can be concluded that Wireshark is a better tool due to multiple reasons such as being open-source, free, and able to use on multiple operating systems. Wireshark is a good tool as it supports around 1000 protocols for testing which is significantly higher than TCPdump. Wireshark can Locate hosts running a specific service and is also able to capture UDP traffic therefore these extra features and the popularity of the Wireshark tool plays an important role in ranking it higher than TCPdump.

2.4.2. Nessus VS Burp suite

Vulnerabilities	Nmap	Nessus	Acunetix WVS	Nikto	BurpSuite
SQL Injection	√	√	√		√
Improper Error Management	√	√	√		√
Cross site Scripting	√	√	√	√	√
Rogue Servers	√	√		√	
Denial of Service	√	√	√		√
Remote Code Execution		√			
Format String Identifier		√	√		√
IIS.printer		√	√		√

Figure 2 Comparison between Nessus and Burp Suite [12]

Nessus is a vulnerability scanner that can list various vulnerabilities that exist on remote hosts. Provide internal and external scanning. The internal scan is related to the hosts in a specific router. External scanning involves hosts outside the router (remote hosts). Web application testing is also performed on the scanner. Nessus is based on a client-server architecture. Each session is controlled by the client and the test runs on the server. More than 100 websites were scanned with Nessus. Nessus not only lists these vulnerabilities but also clearly describes them in detail through thousands of plugins that are regularly updated [13].

Burp Suite scanner performs the scanning of the hosts. With the trial version, The Scanner feature is not available. A full professional version needs to be purchased to perform the scanning. Scanning involves testing the hosts for the vulnerabilities present in them. It identifies the type of vulnerability and its severity. Burp Suite can spider websites very quickly, and most of the pages on the website can usually be found. Once you launch a website, it allows you not to attack any pages you find during the scanning process. This is very useful when you do not want to attack certain parts of the website. The interface is a big problem: no matter how many functions a software gives you, if the functions are not well presented, you will lose most of them when you need them. The presentation of the software should be improvised and more expressive. [12] [13].

Overall, according to the research conducted it can be deduced that Nessus is more widely known as a vulnerability scanner and it can be used in multiple operating systems. This tool is also free to use while Burp Suite requires the paid version to perform complex tasks. Nessus tool is user-friendly and the tool is easier to understand compared to the Burp Suite.

2.4.3. Shodan VS ZoomEye

Shodan.io is a search engine that is specifically designed for IoT devices. Shodan is a useful tool at the initial stage of testing. Moreover, allows intruders to quickly check how a given organization looks like as far as the Internet is concerned. It identifies the invisible parts of the Internet most people will not ever see. Any connected device can show up in a search, such as servers, printers, webcams, traffic lights, Security cameras, Control systems. The engine immediately looks for systems that match your query in terms of vulnerability, affiliation with a given organization, the type of protocol used, location, and many other criteria. All of this can be performed without sending even a single ping towards the target system. Shodan can help penetration Testers to find valuable information about the target. or all ports within the internet can help enterprises identify and lock down security vulnerabilities [7].

Zoomeye is an alternative search engine that is primarily used to view open devices that are vulnerable, and according to the Ethical Hacking Course, penetration testers use them most frequently to test or exploit their vulnerabilities on the Internet. Zoomeye allows users to find specific connected network devices. Zoomeye is a search engine based in China. Zoomeye uses Xmap and Wmap to search for network devices connected over the Internet. These two engines are used for inspections 24 hours a day, 7 days a week. Zoomeye works like any other search engine, you only need to search for queries on the Internet. [14].

Overall, according to the research conducted Shodan is the most preferred search engine among the 2 compared. Shodan is IOT based search engine that is free for performing basic searches however if Some Shodan dorks need to be used then a free account could be created. Shodan is also an open-source search engine that could be compatible with multiple operating systems. Shodan search engines are easy to use and understand. Therefore, Shodan is rated higher and preferred by the people trying to perform reconnaissance. Many such search engines are being created by several countries however these are the two most popular among web users and the people in the IoT industry.

3. RESULT AND DISCUSSION

3.1. Secure Website (Facebook)

In this research of Reconnaissance for the Secure website, Facebook has been considered as the target website. There has been made use of multiple tools for which the desired output is given below. Some of the tools used are IP lookup, Shodan, Nmap scanner, and website vulnerability scanner.

3.1.1. IP address

Figure 3 Ping command on Cmd

The above image shows the IP address of the target website which is Facebook. When the command "Ping" is used it also shows the connectivity and proves that it is up and running. This is one of the main steps performed in the reconnaissance process by the attacker. The IP address is important to perform other tests or any scan.

Figure 4 IPLookup

This is one of the Open-Source tools that could be used to identify the location of the Webserver Hostname, Decimal value and other important details are found using this tool. This information can help generate ideas on how to proceed with Reconnaissance.

3.1.2. Shodan.io

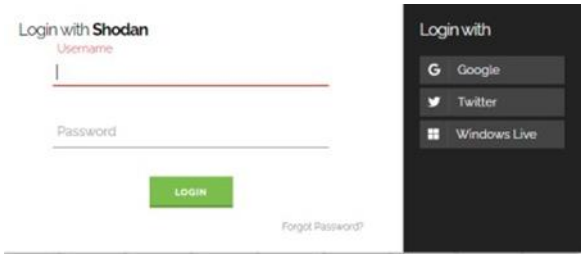

Figure 5 Login in Shodan

This is the login Page for Shodan this is a free account that can be created. This is important to log in so that some advanced features could be used. This feature will help in performing the Shodan dorks

Figure 6 facebook.com

This is the output that is obtained when the URL of the website is facebook.com. Basic information of the ISP, when was the website last updated, Hostname. These are important so that the website is updated regularly and make sure there are no security issues.

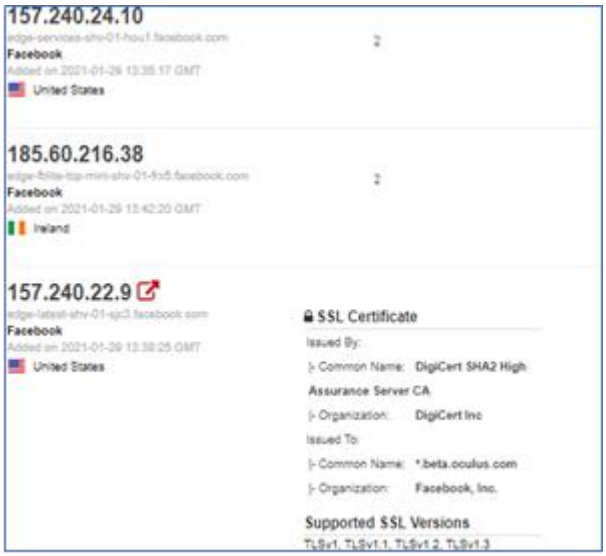

Figure 7 Hostname:facebook.com

This is one of the popular Shodan dorks Hostname:facebook.com. This shows that the IP addresses of the same website in different countries are different. This is a piece of important information and we can also

see that there is an SSL certificate present for this website which means it is secure and there is also some encryption that is present.

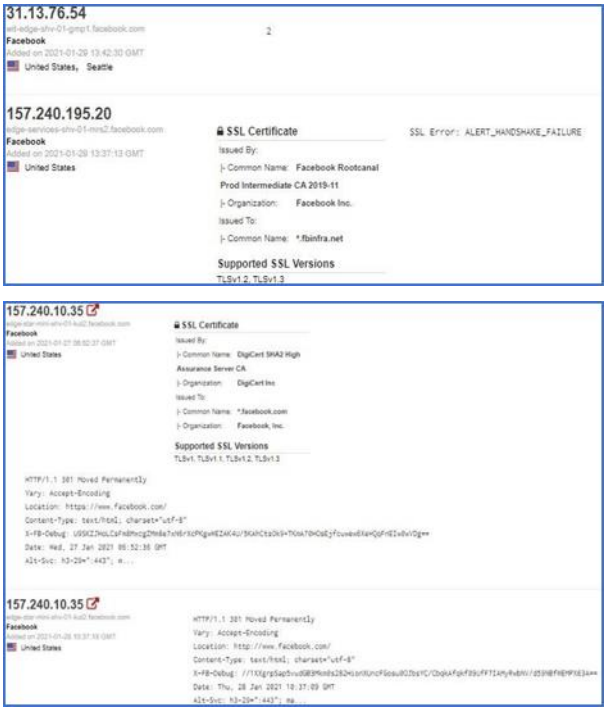

Figure 8 Net:157.240.10.35

This is another Shodan dorks that can be Net: "IP address". This gives details of the HTTPS it is important in understanding the website details. Location and the date and time are also provided for when the website was last updated. The SSL details like who issued also can be obtained.

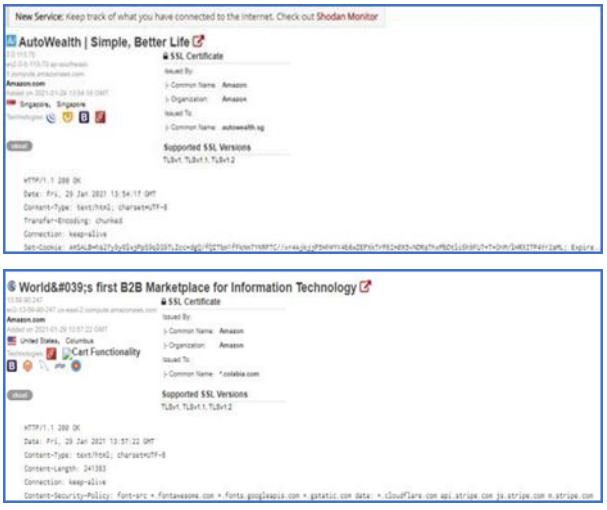

Figure 9 Company's associated with Facebook

The above figure uses another Shodan dork to filter the information available. This also provides information related to company's that are related to Facebook. This can also be useful in some ways. We also get cookies present with these websites and this also can be helpful.

3.1.3. Nmap Port Scanning

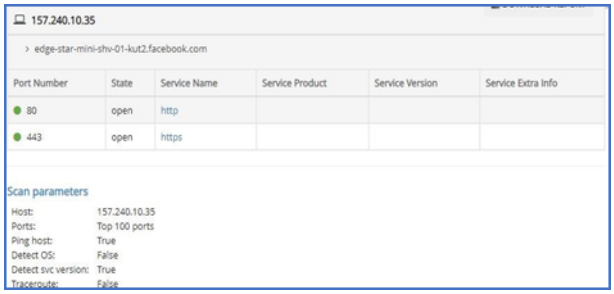

Figure 10 All port scan

Port Scanning was conducted on the target website. Port number 80 and port 443 are open. This shows that the website is secure as HTTPS (HyperText Transfer Protocol Secure) is open. However, this needs to be monitored so that the open ports are not exploited.

3.1.4. Website vulnerability scanner

Figure 11 Run scan

This is a free website vulnerability scanner known as a cybersecurity web test. The URL of the website needs to be entered so that the scan on the website can be conducted. The scan takes about 2 minutes and then a scan report is generated. This is a free version that performs the minimum scan while the paid version provides a detailed report.

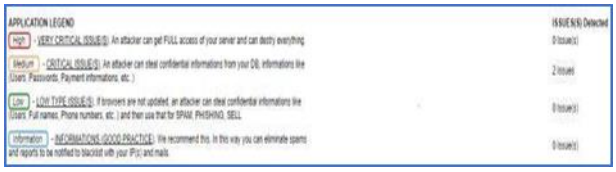

Figure 12 Type of vulnerability

This is a scan report obtained for a secure website Facebook, therefore, medium issues are found however this could be an issue and the safety of the users is at risk, so it must be also rectified and updated from time to time to reduce the risk of any serious attacks.

Figure13 Clickjacking and XSS header

These are the types of vulnerability that have been identified accordingly. How to fix it can be understood by using the advanced paid version. Clickjacking is a type of attack in which the attacker deceives the user into clicking something that might help perform the attack. This is commonly used in websites that are used by many people.

Another important vulnerability that needs to be addressed is the ross-site-scripting attack. It is a type of injection in which the malicious scripts are injected into the otherwise benign and trusted website. XSS attacks occur when an attacker uses a web application to send malicious code generally in the form of a browser-side script [15]. This type of attack has become common and increasingly popular among attackers. The necessary precautions must be taken so that the user data and other important information are not compromised. Organizations like Facebook need to take extra care of such issues that can easily be identified by even free tools. Overall, there is a much fewer vulnerability that has been identified compared to a vulnerable website.

3.2. Vulnerable Website (hackthissite)

In this research of Reconnaissance for the vulnerable website, hackthissite has been considered as the target website. This website is one created especially for trying out website hacking and to identify web vulnerabilities. There has been made use of multiple tools for which the desired output is given below. Some of the tools used are IP lookup, Shodan, Nmap scanner, and website vulnerability scanner.

3.2.1. IP Address

```
Pinging hackthissite.org [137.74.187.104] with 32 bytes of data:
Reply from 137.74.187.104: bytes=32 time=181ms TTL=51
Reply from 137.74.187.104: bytes=32 time=183ms TTL=51
Reply from 137.74.187.104: bytes=32 time=212ms TTL=51
Reply from 137.74.187.104: bytes=32 time=182ms TTL=51

Ping statistics for 137.74.187.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 181ms, Maximum = 212ms, Average = 189ms
```

Figure 14 Ping Command cmd

The above image shows the IP address of the target website which is hackthissite. When the command “Ping” is used it also shows the connectivity and proves that it is up and running. This is one of the main steps performed in the reconnaissance process by the attacker. The IP address is important to perform other tests or any scans.

Figure 15 IPLookup

This is one of the Open-Source tools that could be used to identify the location of the Webserver Hostname, Decimal value and other important details are found using this tool. This information can help generate ideas on how to proceed with Reconnaissance. In this case, the details of the vulnerable website have been gathered. The location is in France and the ISP (internet service provider) is OVH SAS. Information regarding the type of IP address can also be gathered.

3.2.2. Shodan.io

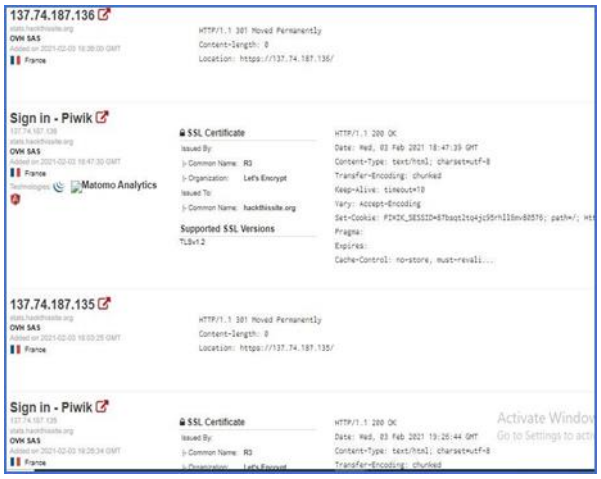

Figure 16 Hostname:hackthissite.org

This is one of the popular Shodan dorks Hostname:hacthissitfe.org. This shows that the IP addresses of the same website in different countries are different. This is a piece of important information, and we can also see that there is an SSL certificate present for this website present. There is no last updated date present which can also mean that website is not secure or up to date.

Figure 17 Net:137.74.187.104

There is not much extra information present however the details specific to the IP address are obtained. There are also some cookies present for this website that could be used to exploit. This information can help gather details of the website user. Therefore, an attacker needs to make use of the cookies, so the user needs to be careful.

3.2.3. Nmap Port Scanning

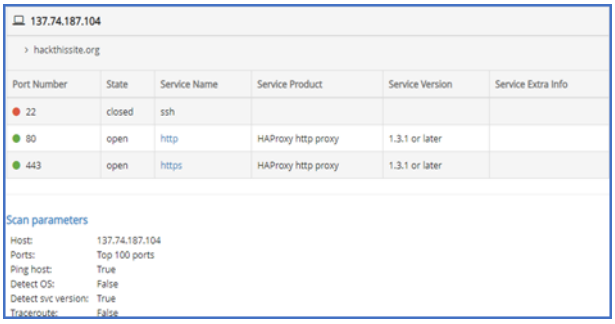

Figure 18 Port Scanning

Port Scanning was conducted on the target website. Port number 80 and port 443 are open. This shows that the website is secure as HTTPS (HyperText Transfer Protocol Secure) is open. However, it is important that this needs to be monitored so that the open ports are not exploited. There is also another port 22 that is closed so it shows SSH services are sometimes performed on this website. SSH is not a secure method to transmit the data remotely so this can be dangerous.

3.2.4. Website Vulnerability Scanner

Figure 19 Run scan

This is a free website vulnerability scanner known as a cyber-security web test. The URL of the website needs to be entered so that the scan on the website can be conducted. The scan takes about 2 minutes and then a scan report is generated.

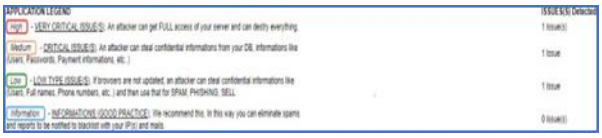

Figure 20 Types of vulnerability

This image shows the types of the vulnerability, so an issue has been detected as there is a high-risk vulnerability detected which is a major issue that means that the website needs attention and needs to be looked upon as soon as possible.

Figure 21 Server details

This image shows the server details which shows there are no issues now however the severity is high if there is any information is leaked so therefore it is important to protect the server data.

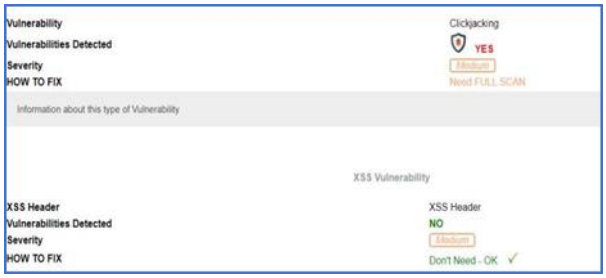

Figure 22 Clickjacking and XSS header

Based on the above image it can be identified that this website is vulnerable to clickjacking and it has been detected. There are no XSS header issues. This clickjacking weakness can play a serious issue in the security flaws of the website.

Figure 23 HTTPS

There are some issues related to the HTTPS protocol. This is a scan for which the results could be identified via the full paid version it is important to make sure that this is checked because the severity of this vulnerability is high.

Figure 24 Form vulnerability

There is a vulnerability that has been detected. This needs to be given attention however small this is an attacker can gather further information and can exploit this easily.

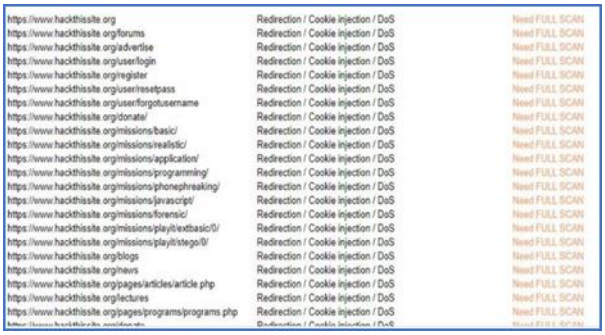

Figure 25 Cookies injection and dos

These are the other potential vulnerabilities related to this website that could be detected upon further scanning. These scans should be conducted by an organization so that it is detected. This is expected for such a website as it is a vulnerable website.

3.3. Critical Analysis

3.3.1. Limitations in Current scenario

In recent times, many companies have established themselves through the internet. The world is fast changing. The COVID-19 pandemic has forced many companies, big and small, irrespective of the size to venture online for survival. These companies can be from different industries such as Banking, Airline, telecommunications, E-commerce, and many others. Not only information regarding the website even personal information or information regarding the company could be gathered. Due to the short period for the implementation process, many companies have not evaluated the potential risks involved in the information that goes online through the company website. Various details such as personal information, company information, financial data, and even information that might help in the further hacking of websites could be gathered by miscreants. Since the companies are startups or new in the venture, they have not allocated a sufficient budget for data security. It is a well-known fact that this pandemic has kept many individuals indoor with access to the internet 24 hours a day. We also have many hacking websites available that can teach youngsters or even kids to learn the basics of hacking and collecting data. This has become a play for some individuals, and it could also lead to major consequences in the long run.

The necessary precautions need to be implemented into any online website. They are vulnerable to many attacks that might affect not only the organization even the trust of the users and the personal information provided might be affected. There needs to be regular checks and tests on various aspects that need to be done. All the new and updated standards need to be applied by an organization so that the risk of attackers is reduced as much as possible. Everything today even small transactions take place online therefore information on the internet is vulnerable to different types of attacks.

3.3.2. Counter measures

Many different types of Cybercrime take place. Countermeasures are actions, procedures, or techniques that are implemented to reduce the threat, vulnerability, or attack by eliminating or by preventing the harm it can cause. In this case, some Countermeasures are mentioned to prevent website hacking. These steps and Measures Could be implemented in all websites so that the websites are secure and safe from any risks that might arise in the future. Some of the measures are mentioned below as follows:

1. The main important thing is Securing the IP address. This needs to be safeguarded. There could be the use of encryption and multifactor authentication that could be implemented so that the IP spoofing and other malicious activities could be minimized. All most every device or website in a network has an IP address so therefore following this step would be vital in all the scenarios.
2. One of the important and simple measures that could be implemented for the website is HTTPS. One of the main benefits of HTTPS is that it adds security and trust. It protects users against man-in-the-middle (MitM) attacks that can be launched from compromised or insecure networks. Hackers can use such techniques to steal your customer's sensitive information [16].
3. Another simple measure that could be implemented is Conducting port scans regularly to check for the services that are open and don't have any use. If these services are unnecessarily open and unattended, they could be exploited by the attacker, so this is important for a website. Popular and frequently used websites tend to have multiple services running simultaneously so it needs to be checked.
4. The Web servers and the CMS (Content Management services) must be updated and patched up regularly. These are some of the vital applications and files which help run the website. If these services are not updated, then the vulnerabilities present with the older versions could be exploited. Moreover, a web application firewall could be implemented to increase the security of the website. Therefore, there must be patches updated at regular time intervals to reduce the damage caused [17].
5. It is also important that an SSL certificate is present for the website as a security measure and if there needs to be any remote data transmission within the website that needs to take place Telnet could be used instead of SSH. This will all help reduce the risk put forward to the attacker.

4. CONCLUSIONS

In this article, the focus is on the important process known as reconnaissance which is a vital step in the website hacking process. Different types of reconnaissance processes are involved to gather the essential information. After extensive research, it has been noticed that the COVID-19 pandemic has highlighted the seriousness of data security breaches that could be potentially dangerous in the online world. There are many free online tools with guides on how to use is available even to amateurs who are looking to extract information for their benefit. This has become a serious threat to the personal information of individuals as well as the company. It is important to allocate a budget and hire experts who will be able to protect the information that might be vulnerable to threats.

Therefore, companies can implement some security measures such as SSL certificates, closing of ports when not in use, and having website services updated regularly to reduce the threats present. These are some of the measures that could help protect the websites. There is a lot of competition present in the world, so everyone tries to take the easy step. It can be concluded that reconnaissance is an important step taken in the process of website hacking. Through the research, it was established that multiple free tools can be used to perform the reconnaissance. It is important to always keep a watch on attackers and make sure that the websites are implemented with the necessary security measures at regular periods.

ACKNOWLEDGMENTS

The completion of this undertaking would not have been possible without the participation and assistance of various authors that have contributed to this topic and as well as Dr. Vinesha Selvarajah. Their contribution is sincerely appreciated and gratefully acknowledged. Without the help of these people, this entire writeup could not have been completed on time so I would like to thank them once again.

REFERENCES

[1] Nishmitha,"Slideshare,"2017.[Online]. Available: https://www.slideshare.net/NishmithaPH/digitalisation-nishmitha. [Accessed 18th January 2021].

[2] M. A. Dennis, "britannica," 2017. [Online]. Available: https://www.britannica.com/topic/cybercrime. [Accessed 18th January 2021].

[3] M. M., "tutorialspoint,"2016.[Online].Available: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_reconn aissance.htm. [Accessed 18th January 2021].

[4] M. Rouse,"techtarget,"2016.[Online].Available: https://whatis.techtarget.com/definition/passive-reconnaissance#:~:text=Passive%20reconnaissance%20is%20an%20atte mpt,determine%20find%20any%20op en%20ports.. [Accessed 18 January 2021].

[5] E. Kaspersky, "Kaspersky," 2014. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a- packet-sniffer. [Accessed 18 January 2021].

[6] g. combs,"Wireshark,"2018.[Online].Available: https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWind owSection.html. [Accessed 18 January 2021].

[7] J. Dzieciątko,"SEORED,"2019.[Online]. Available: https://seqred.pl/en/shodan-improved/#:~:text=What%20is%20it%20Shodan%3F,it%20possible%2 0to%20browse%20them.. [Accessed 18 January 2021].

[8] J.Porup,"CSO,"2019.[Online].Available: https://www.csoonline.com/article/3276660/what-is-shodan-the- search- engine-for-everything-on-the-internet.html#:~:text=While%20Google%20and%20other%20search,im agine%20that's%20plugged%20into%2 0the. [Accessed 18 January 2021].

[9] D. Wendlandt, "nessus," 2017. [Online]. Available: https://www.cs.cmu.edu/~dwendlan/personal/nessus.html. [Accessed 18 January 2021].

[10] L. Obbayi, "infotech," 2019. [Online]. Available: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the- nessus-vulnerability-scanner/. [Accessed 21 January 2017].

[11] G. S. Dr. Charu Gandhi, "Packet Sniffer – A Comparative Study," International Journal of Computer Networks and Communications Security, vol. 2, p. 9, 2014.

[12] J. Gajrani, "research gate," 2014. [Online]. Available: https://www.researchgate.net/figure/comparative-view- of-the-tools- mentioned-above-on-the-basis-of-the-vulnerabilities-these_tbl1_261182006. [Accessed 20 January 2021].

[13] G. jones, "trustradius," 2016. [Online]. Available: https://www.trustradius.com/compare-products/burp-suite- vs-nessus. [Accessed 20 january 2021].

[14] J.Gill,"securitynewspaper,"2018.[Online].Availabl e:https://www.securitynewspaper.com/2018/12/25/

zoomeye-find-open- servers-webcams-porn-sites-vulnerabilities/. [Accessed 4 February 2021].

[15] KirstenS, "owasp," 2018. [Online]. Available: https://owasp.org/www- community/attacks/xss/. [Accessed 13 February 2020].

[16] Paul,"granite5,"2018.[Online].Available: https://www.granite5.com/insights/use-https-vs-http-benefits-switching/#:~:text=benefits%20of%20HTTPS,Security,steal%20your%20customer's%20sensitive%20information.. [Accessed 4 February 2020].

[17] Kramer,"ncsc,"2021.[Online].Available: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos- unternehmen/aktuelle-themen/massnahmen-schutz-cms.html. [Accessed 11 February 2021].