Classifying Malware Cyber Threats using Ensemble learning

Aniruddh Atrey, B.Tech Computer Science Engineering, Amity School of Engineering and Technology (ASET), Amity University, Uttar Pradesh (AUUP)

Dr. Madhulika Bhatia, Professor, Amity School of Engineering and Technology (ASET), Amity University, Uttar Pradesh (AUUP)

Ayush Shrivastava, B.Tech Computer Science Engineering, Amity School of Engineering and Technology (ASET), Amity University, Uttar Pradesh (AUUP)

Prabal Kalhans, B.Tech Computer Science Engineering, Amity School of Engineering and Technology (ASET), Amity University, Uttar Pradesh (AUUP)

ABSTRACT

Right from 2019, when the entire world witnessed a sudden outbreak of an unknown virus, and everything halted, a new kind of boom was seen in the cyber world. Many of the organizations not only shifted from physical to hybrid, but some of them were also able to increase their turnovers. As cyber aspect of institutions grew many folds, cyber attacks subsequently also increased exponentially. This paper elaborates some of the efficient algorithms used for data classification, regression and many more. Cybersecurity is a kind of electronic security over networks that not only helps individuals but also organizations, institutions, and various governmental bodies to safeguard their sensitive data. Artificial Intelligence contains a subset that enables us to develop algorithms which can predict the behavior of many things, this subset is called Machine Learning. Concerned with cybersecurity, we have used few of the ML techniques in this paper so as to implement our planned model, namely K Nearest Neighbor (referred to as KNN), Random Forest Trees, Learning Vector Quantization, Gradient and ADA Boost Classifiers. It is an unsaid thing that today, the world is trying to reach to solutions of various complex problems or issues. For this reason, Ensemble Learning has become a very handy approach in order to reach to the rightmost solution. In ensemble learning we combine various models and experts to reach to a solution

of an intelligence problem. For utmost accuracy there are various steps mentioned in this research that we can take for obtaining the near to perfect results as they involve mathematical formulae. Last but not the least, for the implementation part, there is utilization of various tools such as the BurpSuite, Nikto, OWASP, Metasploit, SQL.

which is a deeper topic of Machine Learning itself.

I. INTRODUCTION

Amidst the pandemic when the world was in lockdown, two things grew to a very vast extent:

1. The number of unicorns in the country.
2. The number of cyberattacks in various forms.

Starting with what cybersecurity is, it is the protection of systems which are connected to the internet, here systems include hardware, software and programs or data. The cyberattacks simply have the aim of misusing and manipulating the data of the user.

A key component of these cyberattacks is malicious software often called as malware which is basically a form of virus that can cause damage to the data of the end user. Nowadays, it comes in various forms. In order to prevent or to get in a safe zone from this kind of attack, machine learning can show its usefulness. Machine learning is mainly classified under two categories, supervised and un-supervised machine learning techniques. Various algorithms of ML can be used, and which can prevent ourselves at an individual or an organizational level from cyberattacks which may ultimately tend to misuse our data. Some of the algorithms used here are:

1. KNN, an algorithm that helps in data classification.
2. Gradient-Boosting, which is again an algorithm based on classification but used under regression.
3. ADA-Boosting, an algorithm present under ensemble learning

II. CYBERSECURITY

The use of the Web and PC programs has altogether expanded throughout the course of recent years, becoming imbued in the present age of clients. Security is turning out to be increasingly more significant as the utilization of PC organizations and applications develops dramatically. Assailants might browse various application ways to wreck devastation on an organization or association.

Network safety centers around three fundamental undertakings: (a) making moves to safeguard gear, programming, and the data they contain; (b) guaranteeing the state or nature of being shielded from the different dangers; and (c) executing and working on these exercises. Individual, administrative, and business information should be shielded from abuse or control by others.

A software capable enough to cause damage to data and systems, is termed as Malware. A Malware is considered as a threatening software for not on the normal people, i.e., individuals, but also the organizations, companies and even the highest of the governing bodies of a country, as there is a lot of private and sensitive data with such kind of bodies. In the recent years, many incidents have been witnessed stealing of information about the credit and debit cards from the monetary portals, stealing of Google's intellectual property, stealing of user's personal property, if we name a few. If we change the course of field where security has been an issue will be the power sector where there have been various attacks on grids and blackouts were witnessed in the

entire city, state, or country.

III. MACHINE LEARNING

Machine learning (ML), a popular subset of artificial intelligence (AI) which utilizes large data sets and identifies interaction patterns among variables and improves through experience. It is a technology which enables computers to learn on their own without actually being programmed for a particular task. Machine learning is the basic essence of artificial intelligence, as it is being used in virtual personal assistants (Alexa, Siri), face recognition, email filtering and computer vision which helps improving their performance with new available data over the period.

Broadly, the approaches in machine learning can be distinguished into two, supervised and unsupervised learning and then there is a third approach which is the hybrid of the supervised and unsupervised learning known as reinforcement learning. Supervised learning is done through a labeled data set, in which the inputs and outputs are defined. The system learns through minimizing the cost function. The learning takes place under human supervision and feedback is required. Commonly, the algorithms used are classification, regression, SVM (support vector machine) and neural networks, they are mostly used as predictive models.

In unsupervised learning the dataset is unlabeled, and the algorithms help in identifying the patterns within the data. The algorithm learns by identifying relations between input and output by itself and it is ideal for pattern recognition as algorithms find all kinds of unknown patterns and cluster them. Few algorithms commonly used are clustering, Convolutional neural networks (CNN) etc. Reinforcement learning is training a model to make a series of decisions, it can reach the desired output by making multiple different decisions. The goal is minimizing the cost function to obtain desired outcome. It is used for autonomous driving, due to which model will be able to make multiple decisions very quickly.

IV. MACHINE LEARNING ALGORITHMS

K Nearest Neighbors: KNN is a grouping strategy wherein all calculation is deferred until after the capability has been assessed and the capability is just privately approximated. Since this method depends on distance for grouping, normalizing the preparation information can fundamentally increment precision assuming the highlights mirror a few actual units or have particular sizes.

Random Forest, likewise alluded to as arbitrary choice backwoods, is a procedure for troupe discovering that can be utilized for relapse, order, and different sorts of work. It works via preparing countless choice trees, then, at that point, utilizing the result from the class to decide the clear method of classes (characterization), or mean expectation (relapse), of each tree. Albeit arbitrary woods habitually outflank choice trees, their precision is a lot of lower than that of slope helped trees. Also, it has been seen that information characteristics influence how well they perform.

LQV: A not very appreciable point of K-Nearest Neighbors is that we have to hold onto our entire created training dataset. The Learning Vector Quantization (or LVQ for short) is an algorithm dealing with artificial neural network and again allows us to choose how many training instances to hold and learns about how those instances must look like.

Gradient Boost Classifier (GB): GB develops an added substance model in a

phase wise forward way; it allows the improvement of any differentiable misfortune capability. Relapse trees of the n classes_ kind are fitted on the negative angle of the multinomial or binomial aberrance misfortune capability at each level. In the specific situation of parallel order, only one relapse tree is produced.

ADA Boost Classifier: An AdaBoost classifier is a type of meta-estimator that starts by fitting a classifier on the dataset that was initially created and then fits additional copies of the classifier on the same dataset, but where the weights of incorrectly classified instances are adjusted in a way that aids in focusing on cases that are challenging.

V. ENSEMBLE LEARNING

Ensemble learning is a method for solving specific computational intelligence problems by carefully generating and combining a number of models, such as classifiers or experts. In order to enhance a model's performance (classification, prediction, function approximation, etc.) or lessen the likelihood of making a mistaken choice of a subpar model, ensemble learning is typically used. Ensemble learning can also be used for error-correcting, selecting optimal (or nearly ideal) features, data fusion, incremental learning, nonstationary learning, and providing a confidence level to the model's judgement. The decision tree classifier and logistic regression were combined for this study's ensemble learner.

VI. ACCURACY MEASURES IN MACHINE LEARNING

The performance evaluation metrics for the attack detection models in this study are True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN). These terms are specified in Table 1.

Accuracy: Ratio of samples classified correctly over the entire dataset

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: The percentage of correctly classified positive samples.

$$Prec = \frac{TP}{TP + FP}$$

Recall: The ratio of correctly predicted positive samples over the total samples of the corresponding class.

$$Rec = \frac{TP}{TP + FN}$$

F1 Score: Harmonic mean of precision and recall.

$$F1 = \frac{2 * TP}{2 * TP * FN * FP}$$

VII. RESULTS

Algorithm used	Accuracy measure
LQV	Precision score: 0.750037884527
	Recall score: 0.5
	Accuracy score: 0.5
	F1 Score: 0.333501595
Random Forest	Precision score: 0.885485494
	Recall score: 0.88484848
	Accuracy score: 0.88484848
	F1 Score: 0.884801707664
KNN Classifier	Precision score: 0.82414085649
	Recall score: 0.8239393934
	Accuracy score: 0.8239393939393
	F1 Score: 0.82391287586
Ensemble Learning	0.83333334
Gradient Boost Classifier	0.835909090909
ADA Boost Classifier	0.8557575757575

Vulnerability Assessment Tools

Burp Suite

Burp Suite is a web penetration testing tool or Web security tool Which is used to perform web security testing for penetration testing with the help of verbs youth we perform, or a penetration testing perform, or a web security tester perform web security testing on web applications. If you are a web security tester, then this is the best tool in cybersecurity. Burp Suite is created by a business named portswigger and is called Burp; it is termed a suite since it has several tools and combines and integrates them all, giving it the name burp suite. Burp Suite is thus named because it contains several cyber security tools, much as how the collection of all test cases gives a test its amusing name. It is capable of performing each and every task you would anticipate a programme to perform in order to conduct web security testing. It contains all the capabilities you would expect a penetration testing tool to have.

The burp Suite contains tabs like proxies, intruders, scanners and more, the process tab is used for intercepting requests and it's a proxy function. So, the Intruder tab contains different attacks which we can perform on a remote website, the way an individual wants to perform a dictionary attack, brute force attack, etc. The scanner module or scanner tab in the burp suite is used for scanning particular websites and its vulnerability. There is one more interesting tab in burp Suite called decoder, so the decoder contains different types of functions which we can use in order to decode a particular thing like URL decode, basic tifo decode and other things.

Burp Suite is available in two versions, the one is pro and the other is free version. So, in the Kali Linux the burp Suite is already installed and it's a free version and if you are a penetration tester then you can use burp Suite with a pro version because it contains more features than the free version. burp Suite is freely available for Linux Mac and Windows.

How does BurpSuite professional work?

Step 1: Open Burp Suite professional. Shown in fig.1

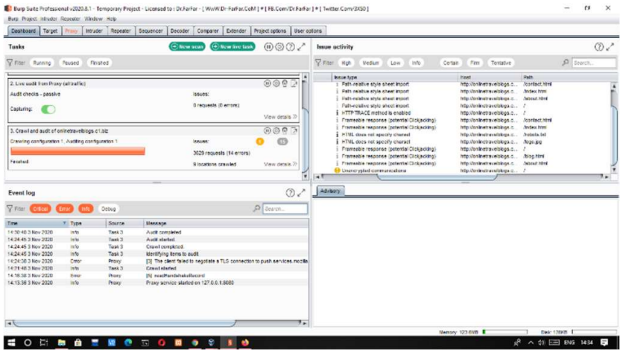


Fig-1

Step 2: Go to the Burp Suite Pro dashboard and click on ‘New Scan’. This opens a scan launcher. Then select the scan type from the top. Shown in fig.2

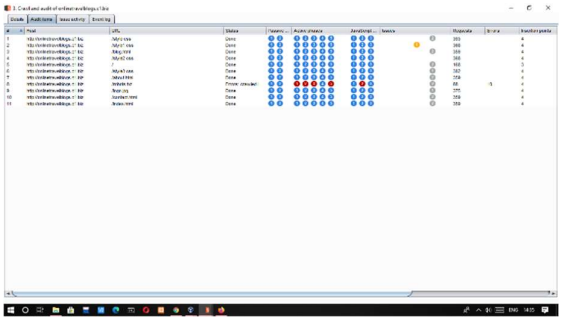


Fig-2

Step 3: Click on crawl and audit which is the default option. Shown in fig.3

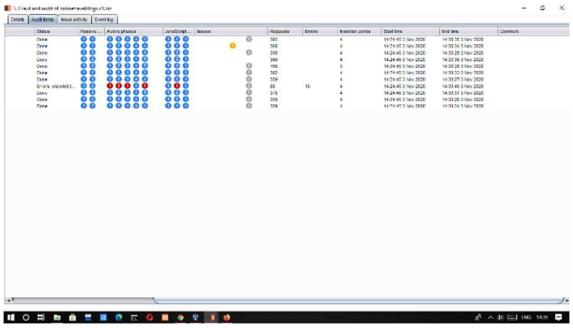


Fig-3

Step 4: After that, enter the URL or multiple URLs to scan. Shown in fig.4

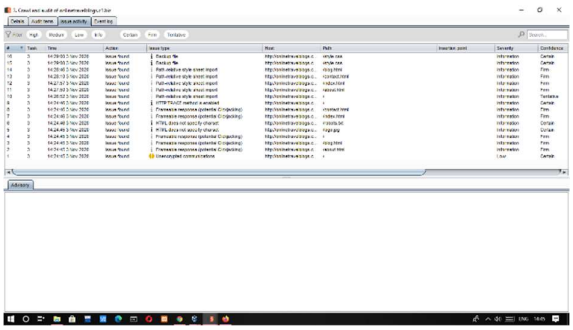


Fig-4

Step 5: Then select scan using HTTP & HTTPS protocol. Shown in fig.5

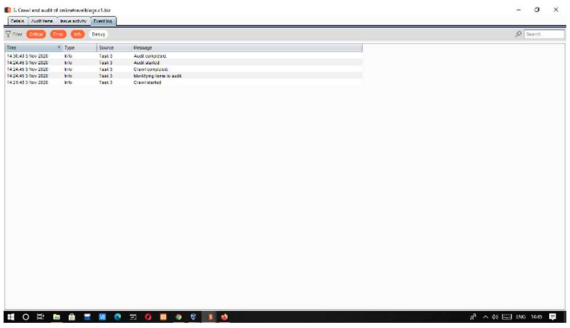


Fig-5

Step 6: At last, click OK. Shown in fig.6

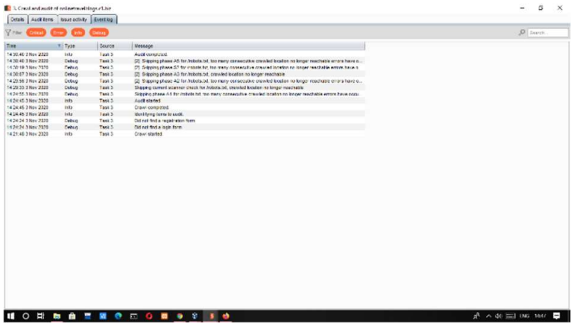
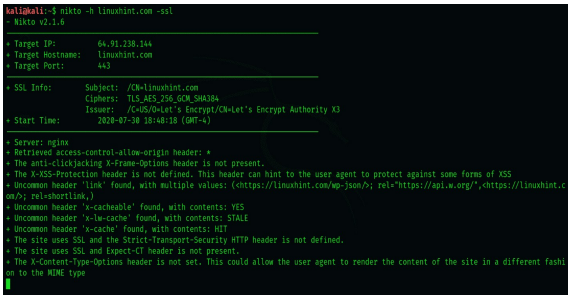


Fig-6

It will start scanning the website and will identify the vulnerabilities of the website. The tool can be optimized as per anyone's need.

Nikto

Nikto is a web vulnerability scanner or a website web server security scanner, it's fantastic for detecting vulnerabilities on the server. necto is generally used by professional penetration testers and web Security Analysis for professional projects because it particularly finds out and detects server misconfigurations, as most of the time system administrators for the people who actually set up website hosting, they really don't know what they are doing, and this comes in the form of of leaving subdomains wide open for people to just find out and furthermore exploit. But finding random server misconfiguration like misconfiguring ports for the get and post comments all of the great Stuff are easily found out by the nikto tool.



Increase in the web application on the Internet today because all the business is now working on an online platform. and internet and online platforms are really required nowadays. It raises the security concerns because in some cases, security is haphazardly considered during development because there are lots of developers, lots of languages and lots of platforms available for different functionalities. As a result, the key is frequently having some online apps that are vulnerable so that attackers can use users' personal information, because lots of things which one is getting from the user side like Bank information phone numbers emails personal data and Company service data can directly land into the hands of the unauthorized.

A web application scanner called Nikto is used by penetration testers, malicious hackers, and web application developers to find security flaws in web applications.

Sullo, CIRT, Inc. originally created, developed, and maintained Nikto. David Lodge is presently responsible for its upkeep, but other individuals have also worked on this project.

How does Nikto work?

Here, Kali Linux was already installed.

So, I did not install anything separately as Nikto is available in Kali Linux.

Step 1: Login to Kali Linux.

Step 2: Then go to Applications. Shown in fig.1

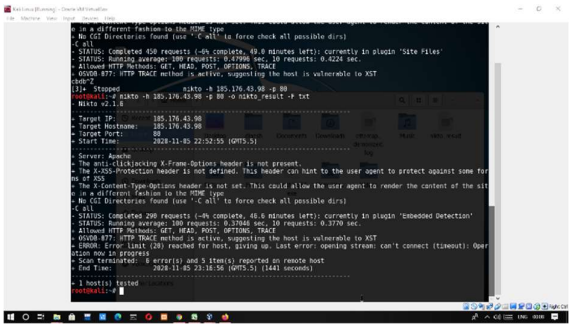


Fig-1

Step 3: Then select 'Vulnerability Analysis' and select Nikto. Shown in fig.2

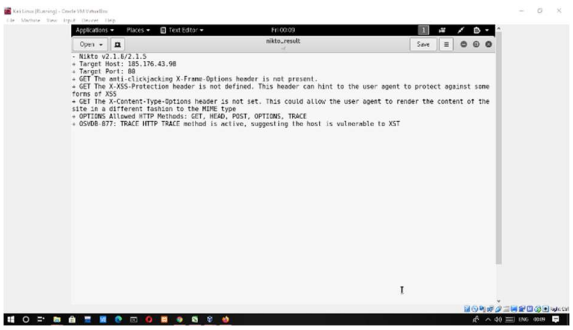


Fig-2

After that, it will open a window or terminal for performing the scan for the web server.

Write a syntax for proceeding with the scan. The syntax used isccccc:

nikto -n $ webserver url

Hit enter.

The mentioned syntax will start the scan and will help us in doing the vulnerability assessment of the website.

Process successfully performed, the vulnerability assessment using these 3 tools. And all I can say is these 3 tools are very effective in website vulnerability assessment.

OWASP- ZED ATTACK PROXY (ZAP)

Finding vulnerabilities in web apps is simple with Zap. It's important to know that you should only use SAP on your own applications, for ones that you have permission to test on. It is completely free and open source. It is one of the select groups of OWASP flagship projects, and it is the tool OWASP recommends for testing web applications. Unlike many security tools, it is ideal for people all new to application security, but it's also used by security professionals, so the IT sector that cgan be used by a wide variety of people. It's also ideal for developers and QA folk, and can be used to create automated security tests that can be incorporated into a continuous development environment. it's also becoming a Framework for advanced testing.

ZAP's Principles

It is free and open source so there is no reason for us to hold back features that other companies decide to charge for. it's also a cross platform tool, therefore, can be used on Windows, Linux, and Mac OS. Each of us is a Priority, which on thinking is important for experts as well as beginners. It's also incredibly simple to install; everything is available in the regular downloads, however it needs Java to function. It has reportedly been translated into a dozen different languages and is considered to be internationalised. There is also a complete set of health files that may be seen online. It integrates well with various tools, allowing you to utilise ZAP in addition to a more specialist tool if necessary.

Zap provides all of the essentials that anyone will need for testing the applications. If someone is new to security then it will probably provide all the features you need, all the professional penetration testers will always want to use a wide range of tools. It functions as an intercepting proxy and is commonly set up to proxy all requests and responses to ZAP. Both active and passive scanners are available. Even though a passive scanner only looks at the requests and their responses, it can nevertheless identify some flaws and vulnerabilities. The active scanner is unique; it executes a variety of attacks and ought to only be used on applications that you have been given permission to test. The programme can be crawled by the spider, for instance, to find pages that have been missed or hidden from view.

How does OWASP ZAP work?

Step 1: Open the Owasp ZAP tool and click on the Quick Start tab.

Step 2: Select the Automated Scan option. Shown in fig.1

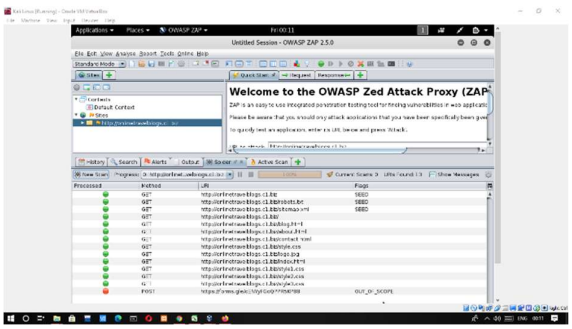


Fig-1

Step 3: Will see a text box where URL of the website whose vulnerabilities have to be found out. Shown in fig.2

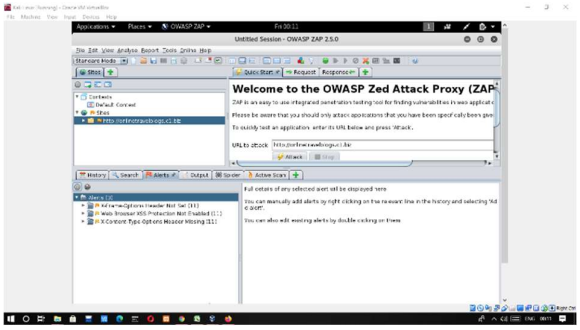


Fig-2

Step 4: After entering the URL, simply click on 'Attack'. Shown in fig.3

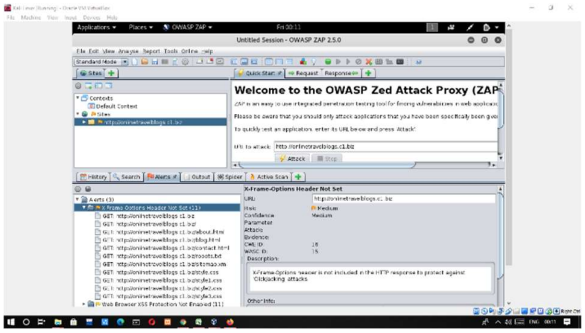


Fig-3

After that it will identify and list the vulnerabilities with the necessary countermeasures. Shown in fig.4 and fig.5

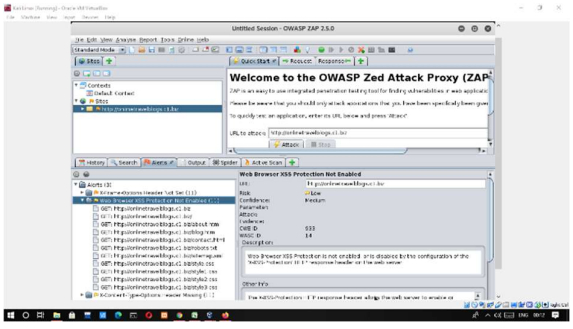


Fig-4

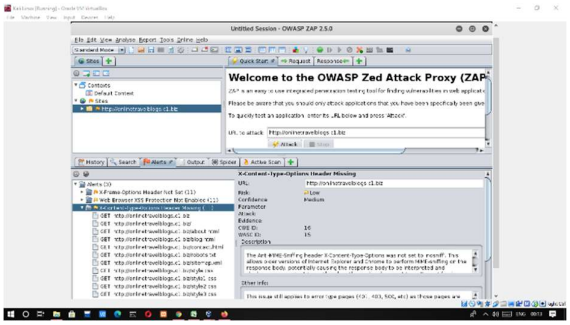


Fig-5

Exploitation Tools

The main idea of hacking, which is the exploitation of the weakness, comes after scanning, information gathering, and locating a vulnerability. The effectiveness of a vulnerability is reduced if it cannot be exploited or if it cannot hurt the application. In order to maximise the impact of a vulnerability, we must exploit it and, frequently, take down a spammer's or hacker's website.

Step 5: The Result Shown in fig.6 and fig.7

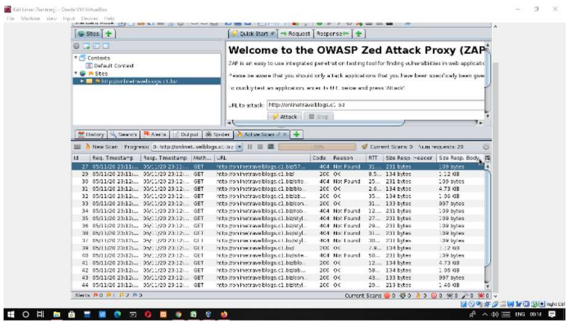


Fig-6

A few of the 300+ cybersecurity and penetration testing tools included with Kali Linux, many of which are used to exploit these flaws, are listed below.

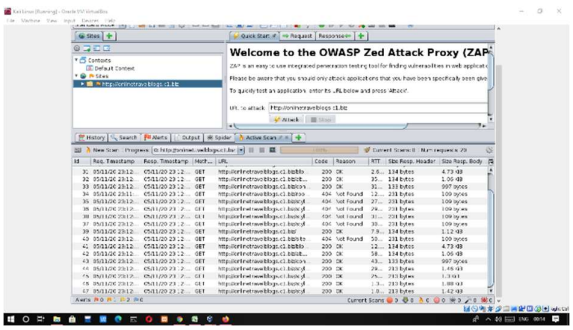


Fig-7

Tools

Metasploit

Metasploit Framework is a tool used for penetration testing, exploit Research and exploiting the system and vulnerabilities in the network. Metasploit Framework is an open-source tool and it's written in Ruby language, which means if someone knows the Ruby language and know how to write codes in Ruby then contribution can be made for Metasploit framework and, Metasploit-framework contains more than twelve hundred exploits, three hundred plus payload, and thirty plus encoders. In Metasploit architecture Metasploit contains many modules such as encoders, exploits, payload, nops and Aux, it also contains libraries such as Erx, MSF Core and interfaces such as console, GUI, web and some plugins.

An exploitation framework, such as Metasploit, is a collection of tools and applications designed to make hacking, system management, and exploit building simpler.

Metasploit real life scenario means how penetration testers use Metasploit in real time in order to exploit or penetrate into the systems, so in order to use Metasploit there are three steps, so the first step is to find open ports services and their version numbers running on the remote version. Once found the open ports and services running on them, then try to find the version of number of services and once we got the version number then we'll try to find exploit in Metasploit Framework database, correspond to that version number which has been found, and if that exploit is present in the Metasploit-framework database then we will use that exploit in order to penetrate that system. Every penetration tester and Security analyst follow this method to achieve success.

Metasploit interfaces are of three types: web interface, GUI interface (Also known as Armitage) and command line interface (MSF console) and it is a cross platform tool hence, it can be used on Windows, Mac, and Linux.

1. Start the PostgreSQL Database Service

PostgreSQL must be started in order to launch the Metasploit framework. This makes it possible for Metasploit to carry out faster searches and save data when scanning or running an exploit. Run the following command after starting the Terminal.

service sudo msfdb init PostgreSQL start sudo (Shown in fig.1)

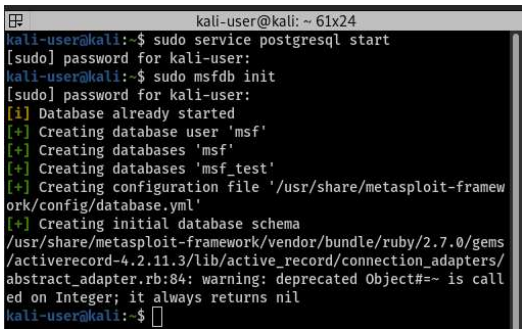


Fig. 1

2. Launch Metasploit

The Metasploit framework has four APIs at your disposal. using MSF Console There are now two methods for starting MSF console on Kali Linux.

- Command-line method
- Graphical Method

Run the commands using the command-line approach on the terminal. (Shown in fig.2)

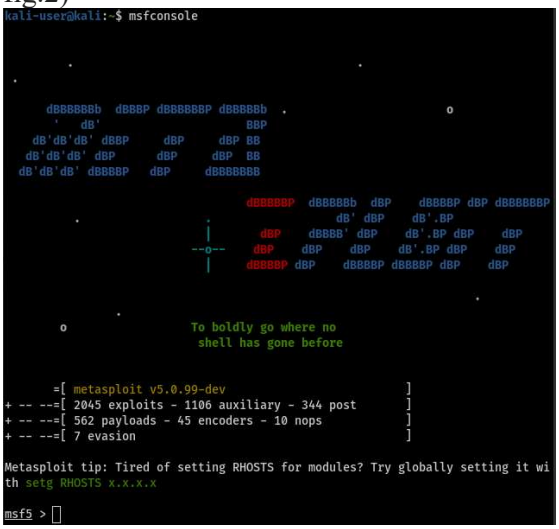


Fig. 2

You can also launch msfconsole from the Kali GUI by selecting Exploitation tools -> Metasploit framework from the Menu button. (Shown in fig.3)

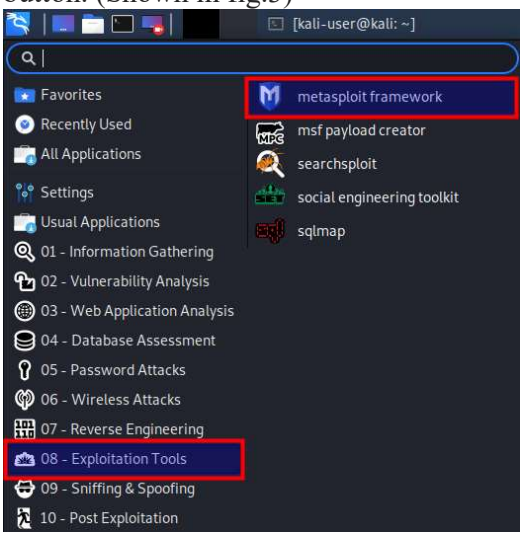


Fig. 3

This will open the Terminal and start the msfconsole command-line shell after asking for the user's password.

Metasploit Tutorial

You will get a Terminal prompt with the format msf[metasploit version] after launching the msfconsole. For instance, in our situation, receiving a msf5 > prompt. That entails using any functional Metasploit versions that may be available. Shown in fig.4

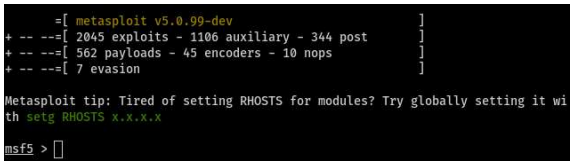


Fig. 4

1. help command

The help command is the first and most fundamental command that everyone should know. Always consult the documentation if you are unsure of your location or which command to use. It displays all the available commands together with their functions. Shown in fig.5

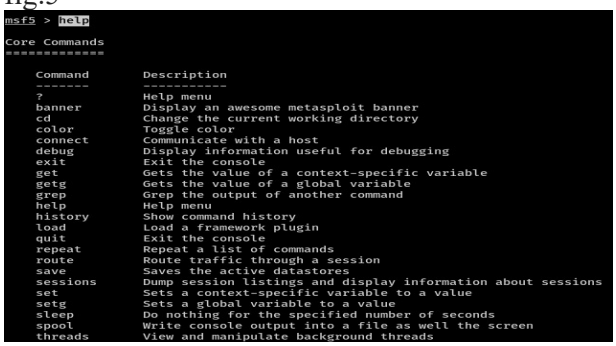


Fig. 5

2. search command

Another helpful tool is the search command. It enables you to search among the hundreds of modules that Metasploit offers. Three parameters can be passed to this command:

- type
- platform
- name

For instance, the technique listed below can be used to look for a typical Unix attack for VSFTPD version 2.3.4. search type:exploit platform:unix vsftpd (Shown in fig.6)

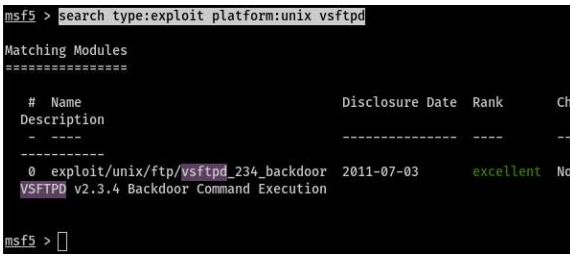


Fig. 6

3. use command

The use command is the second most beneficial command. It enables one to load a module they want to utilise to break into or attack a system. Exploits, payloads, auxiliaries, encoders, evasions, nops, and posts are some of these modules.

Utilizing a module to demonstrate how to take advantage of a vulnerability in VSFTPD version 2.3.4. Run the use command shown below on the msfconsole to load the vsftpd 234 backdoor exploit.
use exploit/unix/ftp/vsftpd_234_backdoor (Shown in fig.7)

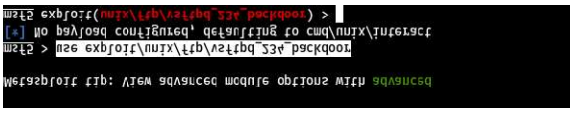


Fig. 7

The prompt will change if the module was successfully loaded at this point. The module's path is added at the end in a different colour (mostly red). There is no cause for concern if the notification "No payload configured, defaulting to..." displays. It signifies that one must manually load the payload because Metasploit is unable to do it automatically. A payload is just the programme or script that is run using the aforementioned exploit.

4. show options command

A module must be successfully loaded before the next command can be executed. Shown in fig.8

show options

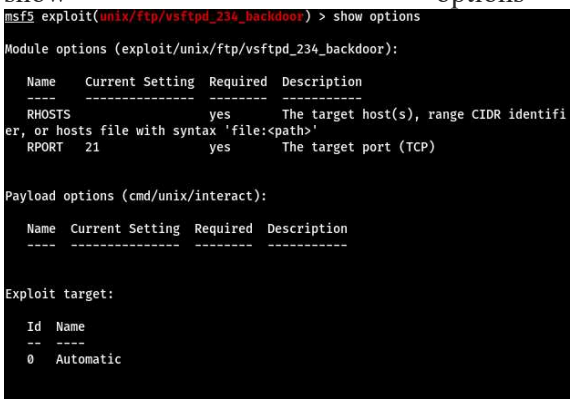


Fig. 8

This command shows the different options that can change with the module. For example, seeing this module requires to set the RHOST and RPORT.

- • RHOST: This is the remote system's IP address, which must be used for exploiting purposes.
- RPORT: That is the target port one is willing to use on the target system.

5. set command

The set command is another useful tool. With this one, you can change the various settings displayed by the show options command. For instance, the following syntax might be used if you want to assign values to RHOST and RPORT.

set RHOST [target_IP]

set RPORT [traget_Port]

e.g
set RHOST 192.168.1.43
set RPORT 21 (Shown in fig.9)

Fig. 9

6. show payloads command

After this, the other command must be executed. The payloads that are compatible with this module are listed by this command.

display payloads (Shown in fig.10)

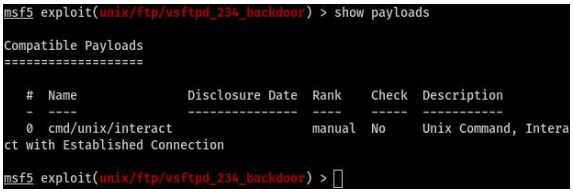


Fig. 10

Only one compatible payload was produced when this command was run on a module. There will be more than 10 compatible modules available for some modules, though.

7. set payload command

The set command can be used to load a specific payload.

set payload cmd/unix/interact

Fig. 11

8. run command

One will be prepared to run the exploit against an existing vulnerability on the target system after the payload has been loaded successfully. The following will be done. Shown in fig.12

run

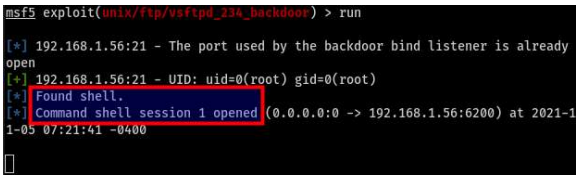
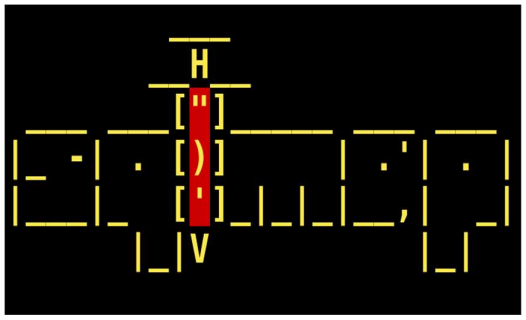


Fig. 12

SQL map



SQL Map Tool is an open-source login testing tool that can be accessed from BackTrack 5 distro or Sourceforge. This tool is used to detect and apply SQL injection errors. It can perform many functions. The top ten OWASP errors of 2010 prioritize SQL injection errors, and SQL injection can lead to a variety of problems, including data loss or corruption

and complete system capture. Hql Map handles stored fingerprints, data downloads, access to subtitle files, and off-band command creation. SQL map software can be used on all OS applications, such as Windows, Mac, and Linux, and on Android phones with termux.

Starting with SQLMAP

All aspiring and experienced ethical hackers favour Kali Linux OS, which is pre-installed with SQLMAP. However, the programme can still be used to install SQLMAP on other Linux computers running the Debian OS.

sudo apt-get install sqlmap

Usage

utilising a website for demonstration purposes that is built with vulnerabilities:

http://testphp.vulnweb.com/listproducts.php?cat=1

The user can alter the value of a GET request parameter (cat = 1) by changing the value of cat. As a result, this type of SQL injection may be possible on this website.

Using SQLMAP, this will be tested. Enter the following in the terminal to view the list of arguments that can be passed:

sqlmap -h

Basic parameters of the SQL commands have been discussed. Along with these, –dbs and -u parameters will also be used, the usage of which has been explained. Shown in fig.1

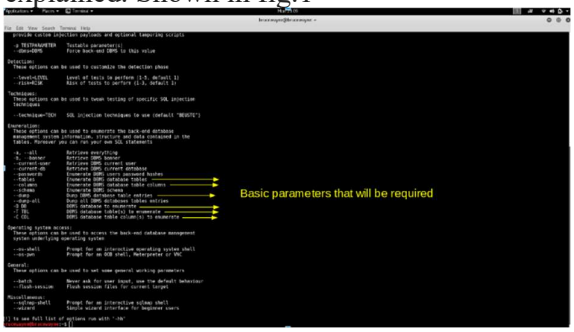


Fig. 1

Testing a website for SQL Injection vulnerabilities with SQLMAP

Step 1: Compile details about the current databases

First, enter the test web url and the -u parameter. -tor is a possible option if you want to employ proxies. Check the website's accessibility now generally. To do this, use the -dbs option. All sites are listed via the -dbs option.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs (Shown in fig.2)

Fig. 2

Two databases are readily available, according to the outputs. The application may occasionally ask the user whether they want to explore different sorts of databases after notifying them that it has located the

database. "Y" is the yes key. Additionally, it might be used to test additional risk criteria, such as type
Here, “Y” has been written because of testing purposes. Shown in fig.3

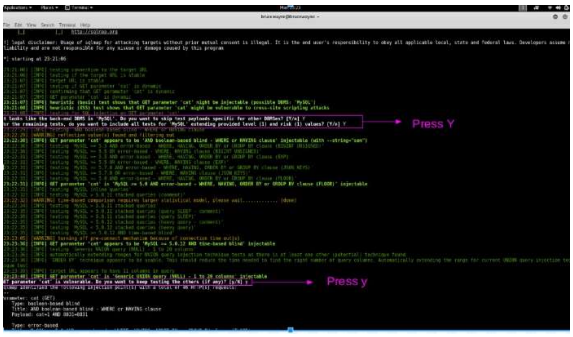


Fig. 3

There are two databases: acuart and information schema, as you can see.

List the details of the tables that are accessible in this specific database in step two.

One needs slightly alter the order in order to attempt to access any website. Now use -D to provide the website's name to access, and after doing so, concentrate on the website's access for tables.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
-D acuart –tables (Shown in fig.4)

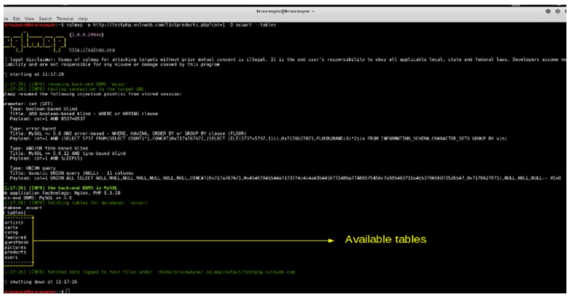


Fig. 4

In the picture provided, 8 tables have been restored. So, the website is vulnerable of the data breach

Step 3: Provide details about each column in a particular table.

Use -T to specify the table name, as previously shown, and word columns for query column names to view the columns of a certain table. One may attempt to approach the "artists" table.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
-D acuart -T artists –columns

Step 4: data from the columns to the trash

Similar to that, you can obtain data in a specific column by using the commands below, where -C can be used to provide the name of the majority of comma-separated columns and the dump query delivers information. Shown in fig.5

Fig. 5

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
-D acuart -T artists -C aname –dump (Shown in fig.6)

Fig. 6

From the image above, inference of accessing data can be observed. Similarly, on such endangered websites, one may be able to perform a 'search of the site' in order to provide information

VIII. CONCLUSION

In this paper, the methods of cybersecurity in machine learning are proposed with the outputs attained from the mathematical equations provided above with the available resources. Right from defining what cybersecurity is and coming to cyberattacks of various forms this paper suggests the users about various prevention techniques under the field of ensemble learning which is further a subtopic of Machine Learning.
Here the algorithms used were LQV, KNN, Random Forest, Gradient Boost, and Adaptive Boost.

IX. REFERENCES

1. Sornsuwit, P. and Jaiyen, S., 2019. A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting. Applied Artificial Intelligence, 33(5), pp.462-482.
2. Haque, M. and Alkharobi, T., 2015. Adaptive Hybrid Model for Network Intrusion Detection and Comparison among Machine Learning Algorithms. International Journal of Machine Learning and Computing, 5(1), pp.17-23
3. Maseleno, A., 2019. Design of Optimal Machine Learning based Cybersecurity Intrusion Detection Systems. *Journal of Cybersecurity and Information Management*, pp.32-43.
4. Disha, R. and Waheed, S., 2022. Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, 5(1).
5. Okutan, A., Werner, G., Yang, S. and McConky, K., 2018. Forecasting cyberattacks with incomplete, imbalanced, and insignificant data. *Cybersecurity*, 1(1).
6. Das, A., -, P. and S, S., 2022. Anomaly-based Network Intrusion Detection using Ensemble Machine Learning Approach. *International Journal of Advanced Computer Science and Applications*, 13(2).
7. Zhang, J., Li, Z. and Chen, S., 2020. Diversity Aware-Based Sequential Ensemble Learning for Robust Anomaly Detection. *IEEE Access*, 8, pp.42349-42363.
8. Voeller, J., n.d. *Cyber Security*.
9. Cornish, P., n.d. *The Oxford handbook of cyber security*.
10. Bosworth, S., Kabay, M. and Whyne, E., 2009. *Computer security handbook*. Hoboken, N.J.: John Wiley & Sons.