International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 02 | Feb - 2022 ISSN: 2582-3930

CyberNAUT With SVT (Security Vulnerability Tester)

JSK HEMASHRI
Department of Computer Science,
Centurion University of Technology,
Vizianagaram, Andhra Pradesh

UPPADA ANANDARAO
Department of Computer Science,
Centurion University of Technology,
Vizianagaram, Andhra Pradesh

UTTAM MANDE
Department of Computer Science
Centurion University of Technology,
Vizianagaram, Andhra Pradesh

Abstract - The world is going ahead with this technical and digital era. As the usage of digital systems and things based on AI are much more advanced. The required security for these systems must be advanced. These systems are coming with a lot more vulnerabilities and bugs. To make this as an assessment and give hands on practice for the new learners, this is a platform. This will be an open-source Operating system with some pre-installed applications and framework which will be very useful for basic EH (Ethical Hacking) learners. This OS (Operating System) is a Debian distribution of the latest 11th version with custom User and Root with their own passwords, this will work similarly to another Linux OS. Smooth and Classic like every other OS. This application (OS) will consist of basic applications like ZMAP, SQL Injection, ZENMAP, & framework like METASPLOIT, website crawlers like BURP SUITE (Professional Edition), etc. With this, an unknown/new application of SVT (Security Vulnerability Tester) which is not available in the market, that's what we are developing. This application is designed to reduce the risk of attackers and protect from unauthorized persons system exploitation, networks and technologies. This application will check the website address and will find the vulnerability in the site. The ultimate aim of this project is to build a bootable pen drive which will consist of this OS with pre-installed frameworks, software and SVT application for the beginner/learners of Ethical Hacking.

Index Terms- Cyber Security, Vulnerabilities, Exploits, Operating System, Applications, Distribution, Frameworks, Kernels, Bootable Devices, Cyber Assaults, Data Access, Linux, Firewalls, Anti-Virus, Product, Cookies, Ethical Hacking, Software, Technology.

I. INTRODUCTION

In this article, a stepwise walkthrough for the product called CyberNAUT, defines a person who is living on the dark side of the world looking at the world. With this word we, the people can also relate in the world of Computer Science that means a person who Illegally/Illegally gains access to & sometimes fixes the information in the technical storage device. World is going on the digitalization or cashless transaction so multi-fold. .Even the government and the security services have suffered huge losses and disruptions on the Internet. The advent of the computer to society is an acceptable step towards modern practices but it needs to be better equipped to compete with the challenges associated with technology. New hacking techniques used to hack into the network and security threats that are rarely detected raise the challenge for security professionals to detect hijackers [13]. The defence method mainly affects their network understanding, attacker environment, attacker motivation, attack method, network security vulnerabilities to minimize future attacks [14]. CN-SVT is an application which is used to reduce the risk of attackers and protect against the unauthorized exploitation of system, networks & technologies. An Operating System is the interface between the computer hardware and the end-user. Processing of data, running applications, file management and handling the memory is all managed by the computer OS. Windows, Mac, Android etc. Are examples of Operating systems which are generally used nowadays. Website vulnerability is a weakness through malformations on the website or web application code that allows the attacker to gain some level of control of the site, and possibly the hosting server.

II. OPERATING SYSTEM (OS)

An operating system (OS) is a program that, after downloading the first program, controls all other applications on the computer. Applications use the operating system to make requests for services using the defined application interface (API) interface. Additionally, users can interact directly with the operating system using the user interface, such as the command line interface (CLI) or graphical UI (GUI) [1]. In addition to the operating system, the entire application will need to enter its own UI, as well as the complete code needed to handle all substandard computer features, such as disk storage, network links and more. Considering the large number of available hardware, this could severely limit the size of the entire application and make software development impossible. The Debian Project is an association of individuals who have made common cause to create a free operating system. This operating system is called Debian. Debian systems currently use the Linux kernel. Linux is a completely free piece of software started by Linus Torvalds and supported by thousands of programmers worldwide. Of course, the thing that people want is application software: programs to help them get what they want to do, from editing documents to running a business to playing games to writing more software. Debian comes with over 50,000 packages (precompiled software that is bundled up in a nice format for easy installation on your machine) all of it free [2].

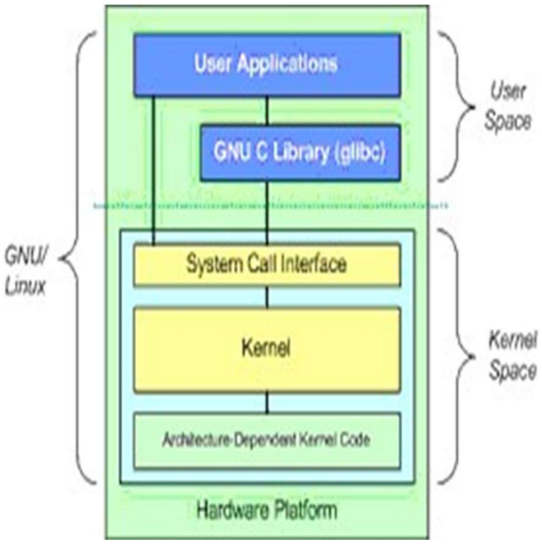
i) KERNEL ARCHITECTURE

Modules or sub-systems that provide the operating system functions. It is the core of an operating system. It is written by C.

The Core Subsystems of the Linux Kernel are as follows:

- The Process Scheduler
- The Memory Management Unit (MMU)
- The Virtual File System (VFS)
- The Networking Unit
- Inter-Process Communication Unit

1. **USER MANNER:** The user interface space in active memory user processes. This memory is beyond the kernel. It includes all accessible memory. Location hidden. The system prevents one process from merging with another process. Only kernel processes can get closer to the user process [11].

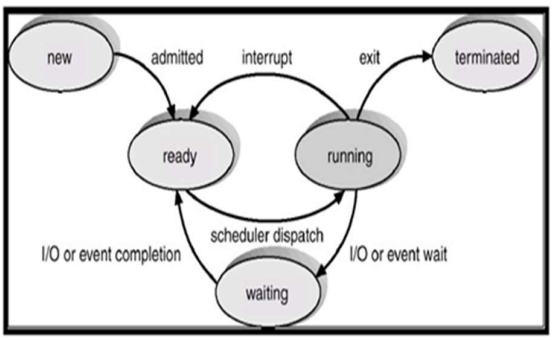


2. **KERNEL MANNER:** A kernel space is a memory space where all kernel servers are provided via the kernel process. Users can only access it via the system. The user process becomes the kernel process when making a system call.

A] Kernel Structural

1. **File system**
   It is responsible for storing data on disk and retrieves and updates this information. File system is accessed through system calls such as: open, read, and write. Example: FAT16, FAT32, NTFS ext2, ext3.
2. **Process management**
   Unix OS is a time sharing system. The whole process usually works for a certain amount of time (a piece of time). Kernel creates, Successes and removes processes [11]

B] Types of Processes



1. **Running:** Process is active or ready to run.
2. **Waiting:** The process is waiting for an event or start.
3. **Stopped:** The process has usually been blocked by receiving a signal.
4. **Zombie:** This is a malicious process that for some reason still has the function of a data structure in 26 vector activity.

C] Device Driver

Related to each portable driver or key driver is a piece of code called Device Driver, which carries the hardware of the device. Key driver functions: Setting hardware in data formatting. It brings connected devices in and out of services. Retrieving data from hardware and transferring it to the kernel. Sending data from kernel to device. Detecting and deceiving device errors.

D] Memory Management

Physical memory is divided into sections of equal size called Pages. The types of memory management are:

- Physical memory.
- Virtual memory.
- Swap memory.

E] Networking :

The first UNIX-enabled communication capability was developed for Berkeley UNIX 4.2 socket sockets based. Sockets provide a networking interface.

ii) LINUX

Applications menu in the top panel in the GNOME area. There are four types of applications to develop applications on Linux.

•GAMBAS Development Environment.
•ANJUTA Development Environment.
•Qt Environment.
•Bluefish editor. [7][8]

i) Advantages of Linux

1. **Cost:**
The most obvious benefit of using Linux is the fact that it is free to find out where Microsoft products are available at a costly and sometimes continuous price. Microsoft licenses are generally permitted to be installed on only one computer, while Linux distributions can be installed on any number of computers without paying a single deck. [7][9]

2. **Security:**
The Linux security feature is much stronger than Windows. The Linux application was able to stay safe in the area of viruses, spyware and adware. The simple advantages of open-source code can establish additional security, liability and performance. Because open-source users are able to quickly identify and fix problems with the system and refer to their development to be included in the system.

3. **Reliability:**
The Linux theme field is higher than Windows because sensitive operating system functions are forced in such a way that batty programs can cause the computer to become unstable and crash.

4. **Capabilities:**
In part of the system, its tools are from the UNIX world, Linux usually comes with an Apache web server, email server, route / firewall capability and SQL information. Linux is not compatible with POSIX which means that applications for Linux can be processed in other POSIX UNIX-sensitive systems with minimal process.

ii) Disadvantages of Linux

- Non-compatible software
- Unsupported hardware

iii) Comparison of Linux, Windows & Mac Operating System

QUALITIES	WINDOWS	MAC	LINUX
Profile Picture #UnhappyGhost			
Simplicity	Very Much	Indeed	Will easily get along
Beauty	Attractive	Impressive	Pretty
Self-Confidence	Still Working on it	Not bad	Yes, indeed
Strength	Easily backs down	Doesn't give up easily	Never gives up
Power	Pumping up	Got some muscles	Super Strong
Financial Mgmt	Spend thrift	Rich dad's spoilt kid	Not demanding
Trust Issues	A lot	Forgiving	Open-minded
Privacy	Very Intrusive	A little	Non-Intrusive
Hobbies #UnhappyGhost	Error pop-ups, BSOD, Crash without warning	Graphics, Designing, Animation	Easily makes friends, parties while other two act sick!
Background Check by CIA (on a funny note...) fb.com/geeksch001	- Acts a good host to malwares - Caught dating Justin Bieber - Recently tried plastic surgery but was a disaster (Win 8)	- Pays Taxes n Bills - Behaves a good citizen. - Fined twice for over-speeding	- Black-Belt in 20 different Martial Arts, - Very high IQ - Killer instincts - No criminal records
Security	Can't count on it	Countable	Nothing like it
Tantrum	Always	Sometimes	Cute indeed!
Heart-Breaker	Big YES	No comments	Will still want it
End Of Day Thought http://unhappyghost.com	I don't want to be in this relationship any more	We can work it out honey	I have more than I deserve!

ii) COMPARATIVES: Here are the highlights of comparison made between the distros of Linux Operating System based on their requirements (hardware), and also on the basics of their interface and their capability to handle the workload [10].

Operating System	Processor Required	RAM	Storage Required
Debian	1 GHz	512 MB	5 GB
Ubuntu	1 GHz	800 MB	5 GB
Kubuntu	1 GHz	1 GB	10 GB
Xubuntu	1 GHz	512 MB	5 GB
Linux Mint	1 GHz	1 GB	10 GB
Slackware	i486	256 MB	5 GB
Fedora	1 GHz	1 GB	10 GB
Red hat Enterprise Linux	1 GHz	1 GB	10 GB
Puppy Linux	333 MHz	64 MB	1 GB
Centos	1 GHz	256 MB	256 MB
OpenSUSE	AMD 64 or Intel 2.4 GHz	2 GB	5 GB

III. VULNERABILITIES

Website vulnerability is a weakness or malfunction of the website or web application code that allows the attacker to gain some level of site control, and possibly a hosting server. Many vulnerabilities are exploited by automated means, such as vulnerabilities and botnets. Cybercriminal hackers create specialized web-based tools to detect certain forums, such as WordPress or Joomla, that require common and published risks. Once detected, this risk is then used to steal data, distribute malicious content, or incorporate malicious content and spam into an endangered site. Possible result. One such type of software is Mat lab. You can readily find M Files related to your research work on the internet or in some cases these can require few modifications. Once these Files are uploaded in software, you can get the simulated results of your paper, and it eases the process of paper writing [3].

i) Accident Leak Information

It is a weakness in web applications where system data or debug information is revealed. This information can be misused and help the enemy to attack the system. Developers of secure systems need to pay close attention to information leaks as they can lead to malicious attacks [15], [16]. All XSS and SQL injection risk tools can be used to obtain any disclosure of information. A notable tool here is Net craft.

Netcraft: is a very popular tool used by security professionals to gather information related to a targeted domain. It can provide great information for footprint testing. As a security expert, this tool can be used to determine what information is leaking to your organization as failure to protect the data collected on your organization's site may expose you to potential attacks. Netcraft uses organization, and sees what you need to fix and what you need to protect from. Netcraft provides web server and web hosting market analysis, including web server and operating system acquisition. It can also say how long the servers have been working, what their duration is, the last time they restarted and more. Netcraft is very easy to use. Users can visit netcraft.com and

set up the domain information they want to get all the details of their intentions [17], [18].

ii) Risk of Cross-Site Scripting

(XSS) risk is a form of injection problem, which means that harmful documents are injected by cyber criminals into trusted web pages. These threats are widespread and occur when attackers use web applications to send malicious codes. In particular, they install browsers in a different end user. Errors in web application development allow these attacks to occur especially when there is a data exchange between users and servers [19], [20], [21]. XSS also exploits the dangers of power-generated web pages. This form can be divided into two subtypes: internal and external:

- **Internal XSS:** is created on the same website where the code will be entered. In other words, hackers will post malicious code as a comment on the website they are shown, such as Facebook or Twitter. In this case, the code will be used and applied to the computer of anyone who opened that injected page or comment.

- **External XSS:** injection can be performed externally using a browser. In this case, the malicious code is not stored on the website, which means that the hacker is the only one who can detect the malicious code

Cybercriminal criminals use XSS to send their malicious codes to targeted users. Malicious script seems to be unreliable because user browsers cannot determine if the requested page is installed and not trusted. As a result, it will generate and execute the text code. Incorrect code can detect cookies and any other important information that a user may send to another party [22]. These scripts can change page content by rewriting HTML. The steps the hackers follow in this attack are:

1) Identify compromised websites and remove required cookies.

2) Generate their malicious code and make sure it will be used in the way they expect.

3) Build URLs. They also could embed the code in web pages and emails.

4) Try to trick users to execute that malicious code, which will end up with hijacking the account or gathering Tunnelling data.

Threats in XSS could be Client-Side Code Injection, Cookie Stealing, XSS Tunnelling, DoS, Malware Spreading, etc. To prevent CSS, we can implement more validations that will take care of those web pages' inputs. Also, we can patch those vulnerable programs. There are infinite tools used to test dynamic web pages, such as XSS Server, XSSer, and OWASP Xenotix. However, these tools could be used by attackers to find vulnerable web pages as well [21], [23].

a) XSS Server: This is server-side loot, which is used to exploit XSS vulnerabilities. The purpose of this tool is to gather sensitive data from users when they execute an XSS code or when they access an injected web page that has embedded XSS code. That victim's sensitive data could be cookies, victim's IP address, web page contents, username and passwords, etc.

b) Cross Site Scripting" XSSer": is an automated framework used to exploit and detect CSS vulnerabilities in web applications. This tool is an open source testing tool that contains many techniques that help pass certain filters. It also has various options for injecting code. XSSer requires Python and runs on multiple platforms [24].

c) OWASP Xenotix XSS: is an advanced framework used for XSS discovery and vulnerability and exploitation. "This tool supports both manual mode and time-based testing methods. Includes XSS encoder, side lock key, and Executable Drive-by downloader". Here are some of the Framework Features of this tool: Xenotix API, Python Scripting Engine with Triple, Payloads, Zero False Positive, XSS Keylogger, Browser Engine Rendering and XSS, XSS Executable Drive-by downloader, and Automatic XSS Testing and Encoder [25]. Unlike other tools, this tool is described as one of the most powerful tools in case of XSS detection and exploitation and can be used to detect most of the XSS threats by performing penetration tests on the web pages against XSS vulnerabilities [26]. The following are some of its features:

- **Payloads:** including HTML5 compatible XSS injection payloads, this tool has more than 380 payloads.

- **XSS Keylogger:** is one way of grabbing users' information that is typed on web pages. The action of recording the keys struck on a keyboard is called Keylogging, which can be used to spy on someone and gain access.

- **XSS Encoder:** This feature allows encoding in different forms, such as URL Encoding, HTML, Base64 and HEX Encoding to bypass web application firewalls and other filters. Moreover, there are many available websites that allow users to generate an XSS code to check their input validation filters against XSS, like XSS String Encoder.

- **XSS Testing:** Xenotix has an automatic testing mode, which tests every payload, based on a period of time that users have to specify according to the needed time to load a web page, which depends on their bandwidth.

iii) SQL Injection Vulnerability

Mostly, databases contain extremely significant information, such as users' credit cards, passwords, etc. Not only database is paramount, but also Database Management System (DBMS) implementation and file system can be affected on the database centralization and distribution. The most common threat in this section is SQL injection which has an ability to shut down the whole system if the underlying file system is modified [2]. Therefore, SQL injection vulnerabilities are widely common, which consist of inserting or" injecting" SQL query via input data" valid statement" from the user to the application. In other words, SQL Injection involves bypassing malicious SQL queries and statements directly to a database through the input fields in the web application in order to access, manipulate, or delete contents [27]. If an injected query is successfully done, its exploitation can read sensitive data, modify it, or even execute administration operations on the database. Moreover, DBMS implementation can be affected by database centralization and distribution. Thus, SQL injection may result in some operating system's error [28].SQL injection allows attackers to spoof IDs and modify current data. As a result, it will cause repudiated issues like changing and rejecting transactions. It can also expose the data on the system or destroy it [29]. Attackers in these types of threats can play as administrators' roles in the database server. In general, the threats of SQL Injection attacks highly depend on the hackers' skills and imagination of the database design and rules configuration [30], [31]. There are many tools used to detect SQL injection, such as SQL Inject-ME, SQLninja, SQLMap, and Havij. However, some of these tools can be used for penetration purposes.

a) SQL Inject-Me: This is an Exploit-Me tool based on Firefox that is used to discover SQL Injection vulnerabilities. It is a suite of tools and applications that is designed to help with application security testing. Users in this tool submit the HTML form and it substitutes the form values with strings that look representative of the SQL Injection vulnerabilities. In fact, it sends database escape strings via those fields in the form then it looks for the error messages that occur as an output. Sql Inject-Me does not make any threats to the system. It works to find any possible way for such an attack against the system, so no password hacking or packet sniffing has been done by this tool. It also does not provide any port scanning or firewall attacks [32].

b) SQL ninja: This is a tool designed to detect SQL injection risks in web applications that use Microsoft SQL Server as its endpoint. The main goal of this tool is to provide remote access to a compromised DB server. It is a very powerful tool, so it can work even in a very hostile environment. When SQL injection vulnerability occurs, this tool should be used to help the tester to take over the DB Server manage the process [33]. Here are some features of this tool:

- Provide a fingerprint of the remote SQL Server, such as its version, user performing the queries, and database authentication mode.
- If the original custom xp_cmdshell is destroyed, it is able to create a new one.
- When there is no TCP/UDP port available, it can do DNS tunnelling pseudo-shell and ICMP-tunnelled shell.
- Brute force of 'sa' password.
- Scan for TCP/UDP ports on the target SQL Server to the attacking machine, to see if there is a port allowed by the target's firewall and use it.

c) Havij: This is an automated tool that helps login detectors to determine the risk of sql injection in web applications. This tool can provide fingerprints for the background website. It is one of the most powerful tools based on the vulnerability of SQL injection due to its unique methods [34], [35]

TABLE: Tools comparison

Tool	Free Source	Feature
OpenSSL	yes	powerful SSL cryptographic library, File encryption and hashing
Qualys SSL Labs	yes	Free, cloud security provider, online
SSLyze	yes	Fast and full-featured SSL scanner, Support StartTLS handshakes
Netcraft	yes	Free, server-side impact, could be used for other types of vulnerability
XSS Server	no	You can generate an XSS script by using this tool
Xenotix XSS	yes	2nd largest XSS Payloads
SQL Inject-Me	yes	No security threats related, can't be installed on Windows 8 and Firefox 19.0.2
SQLninja	no	Successfully tested on Linux, FreeBSD, Mac OS X, iOS
Havij	yes	Friendly GUI, New bypass method for MySQL, automated configuration and heuristic detections

- Obtain data from the DB, dump tables and columns and execute sql statements against the server.
- Ability to recover DBMS usernames and password hashes.

IV. SOFTWARE

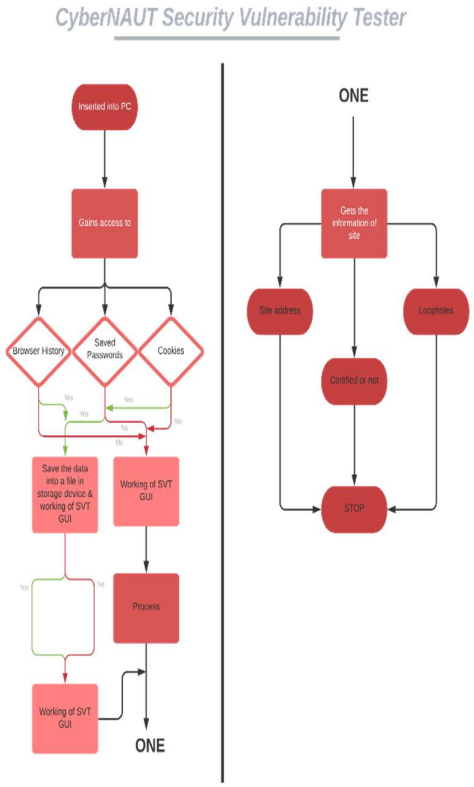
Software is a set of instructions, data, or programs used to operate a computer and execute specific tasks. In simpler terms, software tells a computer how to function. It's a generic term used to refer to applications, scripts, and programs that run on devices such as PCs, mobile phones, tablets, and other smart devices. Software contrasts with hardware, which is the physical aspects of a computer that perform the work. Software vendors provide services in one of four categories: programming services, system services, open source, and SaaS. Vendors generate revenue from software licenses, maintenance services, subscription fees, and support fees [4]. As of 2020, the biggest software companies by revenue are:

- Microsoft
- Oracle
- SAP
- Salesforce
- Adobe

V. APPLICATION

Computer software is basically programs and procedures intended to perform specific tasks on a system. From basic integration languages to advanced languages, there are a variety of software applications. Computer software systems are classified into three major types, namely system software, programming software and application software [6].

VI. PROCESS



The initial working of the system is, when it gets plugged into a system it will gain access to all the information mainly regarding browser history, saved passwords, and the cookies. As the background running executable file has been written in python, which is a cross-platform programming language. There will be three executable files running parallelly when the device gets inserted then a file will be created and all the data will be stored in it. This data will be further used to perform basic Ethical Hacking tasks like session hijacking, password brute-force attacks, and dictionary attacks. In some situations, all three executables might not work but there is an additional GUI based application which will make sure that there is some application which is running when plugged in. The other application is named CN_SVT which will take a website link as an input and provide the details about the website like website name, hosting IP, domain name, etc.

VII. TECHNOLOGY USED

- **Python**
  Python is an easy to read, powerful programming language. It has high-quality data structures and a simple but effective method of object-focused editing. Python's excellent syntax and dynamic typing, as well as its translated environment, make it an ideal language for fast writing and application development across multiple platforms. Python Translator and the general library are available free of charge in the source or binary form at all major forums from the Python website, http://www.python.org/, and can be freely distributed. The same site also contains distributions and references to many free Python modules, programs and tools, and additional documentation. Python Translator is easily expanded with new functions and data types used in C or C ++ (or other C-driven languages). Python is also suitable as an extended language for custom applications.

- **Virtual Box**
  Virtual Box is a powerful product for x86 and AMD64 / Intel64 for business and home use. Not only is Virtual Box an extremely rich product, it works very well for business customers, and it is the only professional solution available as free as Open-Source Software under the terms of the GNU General Public License (GPL) version 2. See "About Virtual Box "of the introduction. Currently, Virtual Box works on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows, DOS / Windows 3.x, Linux (2.4, 2.6, 3.x and 4. x), Solaris and Open Solaris, OS / 2, and OpenBSD. Virtual Box is continuously updated with regular releases and has a constantly growing list of features, supported guest operating systems and platforms in which it operates.

- **Pen Drive**
  A pen drive is a data storage portable device, also referred to as a USB flash drive, consisting of flash memory combined with a USB interface. It enables the user to transfer data like text, videos, images, etc, from the laptop or computer instantly. All that is needed is to plug it in and start dragging-and-dropping files. It is reusable, removable, and smaller than the optical disc. Most pen drives weigh less than 30 g, which is 1 oz. With advanced technology, write drives allow data transfer from one device to another with minimal friction. Pen drives have replaced CDs and floppy disks because they are faster, smaller, are more durable, and have significantly more capacity. It is used for data back-up, storage, and transfer of computer files. A pen drive, often known as a jump drive, uses flash memory modules to store data in a NAND memory format.

VIII. CODE AND EXPLANATION

The data stored in the browser is on the SQLite database. People often use CHROME or FIREFOX as their primary browser which means that most of the data can only be extracted by these browsers. Here we can use the PYTHON forum programming language to do the trick.

- **EXTRACTION OF CHROME HISTORY**

```
import os
import sqlite3
con=sqlite3.connect('/home/[USER_NAM
E ]/.config/google
-chrome/Default/History')
c = con.cursor()
c.execute("select url, title, visit_count,
last_visit_time from urls")
results = c.fetchall()
for r in results:
        print(r)
```

Here is the format of code for extraction of history in chrome. Here the database is connected locally and SQL command is executed thereafter all the results are saved in a variable and data will be saved in the text file.

- **EXTRACTION OF FIREFOX HISTORY**

```
import os
import sqlite3
data_path=os.path.expanduser('~')+"/.mozi
lla/firefox/0mttxac9.default"
files = os.listdir(data_path)
history_db = os.path.join(data_path,
'places.sqlite')
c = sqlite3.connect(history_db)
cursor = c.cursor()
select_statement = "select moz_places.url,
moz_places.visit_count from
moz_places;"
cursor.execute(select_statement)
results = cursor.fetchall()
for url, count in results:
        print(url)
```

Here is the format of code for extraction of history in firefox. Here the database is connected to the history database of firefox and SQL command is executed thereafter all the results are saved in a variable and data will be saved in the text file.

- **EXTRACTION OF COOKIES**

```
import os
import json
import base64
import sqlite3
import shutil
from datetime import datetime, timedelta
# pip install pypiwin32
import win32crypt
# pip install pycryptodome
from Crypto.Cipher import AES
```

Here is the format of code for extraction of cookies in chrome/firefox browser. However, the custom functions will be written to perform tasks like getting date-time, encryption of password, saving the password in a specific path, and decrypting the encrypted password.

- **SAVING A FILE**

```
save_path = '/home'
file_name = "test.txt"
completeName = os.path.join(save_path,
file_name)
print(completeName)
```

Here is the format of code for saving of files in flash storage device

IX. RESULTS AND OBSERVATIONS

As per the observation we can see that when a device is booted up and is ready to use, we can insert the USB Flash-Drive and can extract the required information we needed from the victim's/targeted computer/PC.
The process of extracting the data is very simple,

1. Insert the USB Flash-Drive.
2. Extract the information.
3. Retrieve the data in the required device.

The extracted data is saved in the .txt format i.e readable in any OS.

X. CONCLUSION

By utilizing CyberNAUT- Open source Distribution Framework and the number of applications it supports like Metasploit, I was able to get access on the target Debian Linux machine. Metasploit Framework offers a significant variety of exploits with the collection of all operating systems with available versions and service packs. Specifically in the actual world situation; it is essential to include a complete variety of threats and available most critical categories applications from CyberNAUT. The assessment needs to be carried out on systems with anti-virus and firewalls to get the precise final result. And all those resources need to be utilized which have most recent vulnerability exploits. The overall impact has been the growing list of online attacks, and the corresponding growth in the loss of patients. Although there are few attacks on foreign governments, these threats are worrying because of their potential for harm, when it comes to sensitive infrastructure. Similarly, new buildings may be constructed with minimal risk and damage. We need to expand our global projects so that online crimes can be properly avoided, investigated, and prosecuted without regard to the perpetrators and victims. conclusion. The conclusion may expand on the importance of the work or suggest applications and extensions

REFERENCES

[1] https://whatis.techtarget.com/definition/operating-system-OS

[2] https://distrowatch.com/table.php?distribution=debian

[3] https://www.sitelock.com/blog/what-is-a-website-vulnerability/

[4] https://www.webopedia.com/definitions/software/#vendors

[5] https://www.educba.com/what-is-application-software-its-types/

[6] M. Curphey, D. Endler, W. Hau, S. Taylor, T. Smith, A. Russell, G. McKenna, R. Parke, K. McLaughlin, N. Tranter *et al.*, "A guide to building secure web applications," *The Open Web Application Security Project*, vol. 1, p. 1, 2002.

[7] Linux – Learning the Essentials written by K.L James.

[8] https://www.sics.se/~amir/files/download/oslab/linux1.pdf

[9] http://www.osnews.com/story/24936/Damn_Small_ Linux_Still_Damn_Fun

[10] www.howtogeek.com/.../10-of-the-most-popular-linuxdistributions(29/03/2016)

[11] https://www.sics.se/~amir/files/download/os-lab/linux1.pdf

[12] Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. "Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.

[13] Ahmad, Ateeq. "Type of Security Threats and It's Prevention." Int. J. Computer Technology & Applications, ISSN (2012): 2229-6093.

[14] Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.

[15] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party computer clouds," in Proceedings of the 16th ACMconferenceonComputerandcommunications security. ACM, 2009, pp. 199–212.

[16] M. S. Alvim, K. Chatzikokolakis, A. McIver, C. Morgan, C. Palamidessi, and G. Smith, "Axioms for information leakage," in Computer Security Foundations Symposium (CSF), 2016 IEEE 29th. IEEE, 2016, pp. 77–

[17] N. Ltd. (2015) Netcraft tool. [Online]. Available: http://toolbar.netcraft. com/

[18] A. Bruns, "Prosumption, produsage," The International Encyclopedia of Communication Theory and Philosophy, 2016.

[19] E. V. Nava and D. Lindsay, "Our favorite xss filters/ids and how to attack them," Black Hat USA, 2009.

[20] L. K. Shar, H. B. K. Tan, and L. C. Briand, "Mining sql injection and cross site scripting vulnerabilities using hybrid program analysis," in Proceedings of the 2013 International Conference on Software Engineering. IEEE Press, 2013, pp. 642–651.

[21] S. Gupta and B. Gupta, "Cross-site scripting (xss) attacks and defense mechanisms: classification and state-of-the-art," International Journal of System Assurance Engineering and Management, pp. 1–19, 2015.

[22] D. Catteddu, "Cloud computing: benefits, risks and recommendations for information security," in Web Application Security. Springer, 2010, pp. 17–17.

[23] J. Snehi and D. R. Dhir, "Web client and web server approaches to prevent xss attacks," International Journal of Computers & Technology, vol. 4, no. 2, 2013.

[24] XSSer. (2016) Cross site scripter. [Online]. Available: http://xsser.03c8. net/

[25] OWASP. (2015) Fingerprint web application framework. [Online]. Available: https://www.owasp.org

[26] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, "State of the art: Automated black-box web application vulnerability testing," in Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010, pp. 332–345.

[27] M. Kiani, A. Clark, and G. Mohay, "Evaluation of anomaly based character distribution models in the detection of sql injection attacks," in Availability, Reliability and Security,2008.ARES08.Third International Conference on. IEEE, 2008, pp. 47–55.

[28] S.Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34, no. 1, pp. 1–11, 2011.

[29] H.Shahriar, S.North, and W.-C. Chen, "Client-side detection of sql injection attack," in Advanced Information Systems Engineering Workshops. Springer, 2013, pp. 512–517.

[30] A. Shulman and C. Co-founder, "Top ten database security threats," How to Mitigate the Most Significant Database Vulnerabilities, 2006.

[31] P. Kumar and R. Pateriya, "A survey on sql injection attacks, detection and prevention techniques," in Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on. IEEE, 2012, pp. 1–5.

[32] Imbalife. (2014) How to use sql to inject me. [Online].Available:https://www.imbalife.com/how-to-use-sql-inject-me

[33] A. Singh, Instant Kali Linux. Packt Publishing Ltd, 2013.

[34] S. Pundlik, R. Kumar, B. Gaikwad, A. Aadhale, and V. Waghmare, "Sqjhs: Sql injection attack handling system," in International Journal of Engineering Research and Technology, vol. 2, no. 6 (June-2013). ESRSA Publications, 2013.

[35] B.Nagpal, N. Singh, N. Chauhan, and A. Panesar, "Tool based implementation of sql injection for penetration testing," in Computing, Communication & Automation (ICCCA), 2015 International Conference on. IEEE, 2015, pp. 746–749

AUTHORS

1. **JSK HEMA SHRI** is currently pursuing her second year in Computer Science and Engineering at Centurion University of Technology and Management (CUTM), Vizianagaram, India. She is enamoured with the concepts of Networking, Hacking and Cyber security. At present, she is currently working on a project called CyberNAUT with SVT to reduce the risk of attackers and protect against the unauthorized exploitation of the system.

2. **U. ANANDA RAO is** currently in his second year in Computer Science and Engineering at Centurion University of Technology and Management (CUTM), Vizianagaram, India. He is passionate about the areas related to Hacking, Networking and Expert Systems. At present, he is working on a project called CyberNAUT with SVT to decrease the present threats on the system, networks and technologies leading concepts.

3. UTTAM MANDE received the Bachelor of Computer Applications from Andhra University, Visakhapatnam and proceeded to do his Master of Science in Information Science and Master's in technology of Computer Science and Technology department in Andhra University. He has received his PhD degree in Computer Science and Engineering from CSE department of JNT University, Kakinada, India for his work in the field of. Expert Crime Investigation Systems. He is a member of IEEE and IEEE CS and has organized many workshops and was involved in Research Projects. He has also published several international journals on the subject of Expert Crime Investigation Systems. He is currently working as Associate Assistant Professor, Head of the Department CSE at Centurion University of Technology and Management, Vizianagaram, Andhra Pradesh and his main field of research includes Data Mining and Rule-based Reasoning.