MCT

MANJARA CHARITABLE TRUST

RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI

Versova, Andheri (W), Mumbai-400053

A Synopsis Report

ON

”Cyber-bot” Chatbot for cybersecurity

BY

NIKHIL RAO-747

MOHAMMAD HASNAIN RAJAN-745

VANSHI-740

Under the guidance of

Internal Guide

Mr. Nilesh Rathod

MCT

MANJARA CHARITABLE TRUST

RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI

Versova, Andheri (W), Mumbai-400053

Information Technology

University of Mumbai

Nov. – 2019

MCT
MANJARA CHARITABLE TRUST
RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI
Versova, Andheri (W), Mumbai-400053

CERTIFICATE

Department of Information Technology

This is to certify that

1-Nikhil Rao (747)

2-Mohammad Hasnain Rajan (745)

3-Vanshi (740)

Have satisfactorily completed this synopsis entitled

“Cyber-bot” Chatbot for cybersecurity

Towards the partial fulfilment of the

FOURTH YEAR OF ENGINEERING

IN

(Information Technology)

As laid by University of Mumbai

Guide

Mr. Nilesh Rathod

H.O.D

Dr. Sunil Wankhede

Principal

Dr. Sanjay Bokade

Internal Examiner

External Examiner

MANJARA CHARITABLE TRUST
RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI
Versova, Andheri (W), Mumbai-400053

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violations of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

----

1 Nikhil Rao

----

2 Mohammad Hasnain Rajan

----

3 Vanshi Negandhi

Date:

ACKNOWLEDGEMENT

We wish to express our sincere gratitude to Dr. Sanjay Bokade, Principal and Dr. Sunil Wankhede, H.O.D of Information Technology of RGIT for providing us an opportunity to do our project work on” Cyber-bot” Chatbot for cybersecurity.

This project bears on imprint of many peoples. We sincerely thank our project guide Mr. Nilesh Rathod for his guidance and encouragement in carrying out this synopsis work.

Finally, we would like to thank our colleagues and friends who helped us in completing the Project (Synopsis) work successfully.

1. Nikhil Rao
2. Mohammad Hasnain Rajan
3. Vanshi

ABSTRACT

The objective of this project is to develop an intelligent chat-bot that can take questions about a certain vulnerability selected by the user and give appropriate and suitable answers according to the description of it. The chat-bot takes input from the user about the vulnerability that he/she wants more information about the system then collects the description from sources such as the National Vulnerability Database and answers questions according to the description provided. It has been a huge help for the security analysts as they can find the important details about the report by just asking the chat-bot and getting an instant reply, this has shortened the previous used procedure in which the analyst had to glance through the entire CVE of a vulnerability to find the germane points that was a lengthy and exhaustive task for them.

With the advancement of chat-bots now they can answer to any question within no time, nowadays the chat-bots are voice equipped and have the ability to speak like human individuals. This has helped many businesses to quickly go through any data. Chat-bots are used for a wide variety of applications like analyzing something, interviewing someone, conducting surveys and interacting with customers. This helps to gain insights that makes it easier for any security analyst to better understand a vulnerability.

TABLE OF CONTENTS

List of Figures

CHAPTER 1

INTRODUCTION

As attacks become more targeted and unique, it’s critical that security teams are equipped with the tools required to stop attacks before information theft. Even if teams have the right tools, however, they often lack sufficient resources or expertise to decode the massive number of security alerts hitting their screens daily from multiple point products.

This problem is not going away anytime soon: the cybersecurity workforce gap is on track to reach 1.8 million by 2020. While there’s an urgent need for people to solve the talent problem, there’s also an urgent need to solve for the ‘automation’ problem. How do we equip inexperienced analysts with the power to accelerate attack detection and response?

ABILITY TO UNDERSTAND ANALYST LANGUAGE AND INTENT: Chatbots are powered with natural language processing, a subset of machine learning, that allows them to translate and interpret human language input by pairing natural language understanding (NLU) with security domain expertise to identify analyst intent and guide user workflow. As a result, users of any skill level can ask the chatbot simple questions and receive definitive answers without learning complex and proprietary syntax of multiple point products.

TRANSFORM A TIER 1 ANALYST INTO A TIER 3 ANALYST: Defeating today’s attacks requires analysts to detect malicious behavior across millions of running processes. For inexperienced analysts, this requires them to spend hours - if not days - combing through data and identifying malicious patterns. With The chatbot, analysts can ask “what is suspicious in my network today?” and the chatbot will digest millions of events across endpoints in seconds and provide the user with malicious activities on the network. The chatbot will then guide the user on what to do next to either stop or kill the process. By preemptively suggesting the most urgent information to the user, the chatbot empowers less-experienced Tier 1 analysts to behave at the similar level of sophistication as a Tier 3.

DETECTING IN-PROGRESS ATTACKS: Imagine you work for a large enterprise, and you've just signed a partnership with a company in the UK that requires you to connect them with your company network. Your CEO has just seen the WannaCry ransomware attack in the news, and wants to ensure that the partner has not been compromised with the attack.

ABILITY TO ADAPT OVER TIME: While we believe that AI-powered chatbots are helping to simplify security operations, we know that it's not a silver bullet to solving all challenges in the industry. We also know that machine learning models have limitations, which is why the chatbot has built-in domain expertise and as customers continue to use the chatbot, the bot will learn and adapt to user needs over time. The chatbot is constantly iterating and improving to understand context and patterns in language, and look forward to further feedback from the community.

CHAPTER 2

AIMS AND OBJECTIVES

2.1 AIMS

- To develop an Intelligent Chat-bot that can perform analysis of CVEs given by the National Vulnerability Database and give appropriate answers.
- The main aim of the project is to help user better understand the data quickly and efficiently.
- It is proposed to take input from the users about the vulnerability, help him choose a certain one, gather data form NVD analyze that data and prove an almost real time response to the questions asked by the user

2.2 OBJECTIVES

- To help reduce time for summarizing the CVE description in the NVD of data for analysts.
- The objective of this project is to develop a chat-bot that can give key insights of any vulnerability in no time.
- This project uses BIRT to get the desired results.

CHAPTER 3

LITERATURE SURVEY

1. Cognitive Cyber Security Assistants – Computationally Deriving Cyber Intelligence and Course of Actions. [4] (Charles Palmer, Lee Angelelli, Jeb Linton, Harmeet Singh, Michael Muresan)

   Conventional data analytics process uses dashboard with tables, charts, summaries, search tool in projecting its analysis outcome to its user with the goal of enabling discovery of useful information or suggesting conclusions to support decision-making. Such decision-making mechanisms can be improved further by using natural language interface in the dashboard components, e.g. using natural language keywords to search the sales performance of a product. Motivated by the needs to enable a user friendlier interaction with analytics outcome, this paper proposes a chatbot, called analytics bot who can assist in the role of decision making by delivering information of dashboard components with human like conversational pattern.

2. Cyber Security Assistant: Design Overview [5] (Sayan, Carla & Hariri, Salim & Ball, George. (2017))

   This paper focuses on the design and implementation of an Intelligent Cyber Security Assistant (ICSA) architecture that would provide intelligent assistance to a human security specialist. The ability to focus on rapidly developing malicious events which have the most impact on the normal operations of cyber resources and services is both critical and challenging. Effectively responding to cyberattacks, which have been expanding at alarming rates, will require advanced machine learning to automatically detect attacks and intelligently recommend the mechanisms to render attackers incapable of re-launching new attacks. To effectively address these challenges, we present the design and implementation of an intelligent cyber assistant that will assist security analysts by efficiently and promptly defending cyberspace resources and services against both existing and novel attacks. Additionally, we show that the ICSA can adapt and learn efficiently to improve our intelligence gathering and analytics capabilities to perform sophisticated cyber situation awareness tasks and to develop automated and semiautomated actions to protect against discovered vulnerabilities.

3. An Intelligent Security Assistant for Cyber Security Operations. (C. M. Sayan)

   Our research is initially motivated by a conversation we had with a group of cyber security analysts that are responsible for monitoring enterprise security at a large corporation who were experiencing day-to-day operational burdens. As a result, this paper focuses on the design and implementation of an Intelligent Cyber Security Assistant (ICSA) architecture that would provide intelligent assistance to a human security specialist. The ability to focus on rapidly developing malicious events which have the most impact on the normal operations of cyber resources and services is both critical and challenging. Effectively responding to cyberattacks, which have been expanding at alarming rates, will require advanced machine learning to automatically detect attacks and intelligently recommend the mechanisms to render attackers incapable of re-launching new attacks. To effectively address these challenges, we present the design and implementation of an intelligent cyber assistant that will assist security analysts and ease the day to day operational burdens by efficiently and promptly defending cyberspace resources and services against both existing and novel attacks.

CHAPTER 4

EXISTING SYSTEMS

There aren't particularly similar existing applications that provide the response to key business insights driven through data. Some of the similar chat-bots are:

Endgame's chatbot Artemis™: Artemis is an intelligent assistant that automates security analyst actions and guides users of any skill level to detect and respond to attacks through a simple conversational interface. Just as digital assistants like Siri or Alexa proved their ability to give time back to our day by tackling complex tasks, Artemis automatically combs through millions of data points in Endgame's endpoint protection platform to provide users with definitive answers required to stop attacks faster and earlier than with legacy endpoint products. We know we're biased, but we believe that chatbots have the ability to help solve for the talent and automation problems in our industry by dramatically simplifying complex tasks for security teams.

IBM Hayvn- IBM Security (NYSE: IBM) today announced the availability of Watson for Cyber Security, the industry's first augmented intelligence technology designed to power cognitive security operations centers (SOCs). Over the past year, Watson has been trained on the language of cybersecurity, ingesting over 1 million security documents. Watson can now help security analysts parse thousands of natural language research reports that have never before been accessible to modern security tools.

CHAPTER 5

PROBLEM STATEMENT AND SCOPE

5.1 PROBLEM STATEMENT

There is a rising problem in which the users have to manually analyze vulnerabilities and get the key insights. It is a lengthy and tedious task that often consumes a lot of time which could be saved by using this chat-bot. certain problems associated with chat-bots are:

1. Securing a chat-bot
2. Human like conversational bot.
3. Gathering data via various channels just by giving a single data input

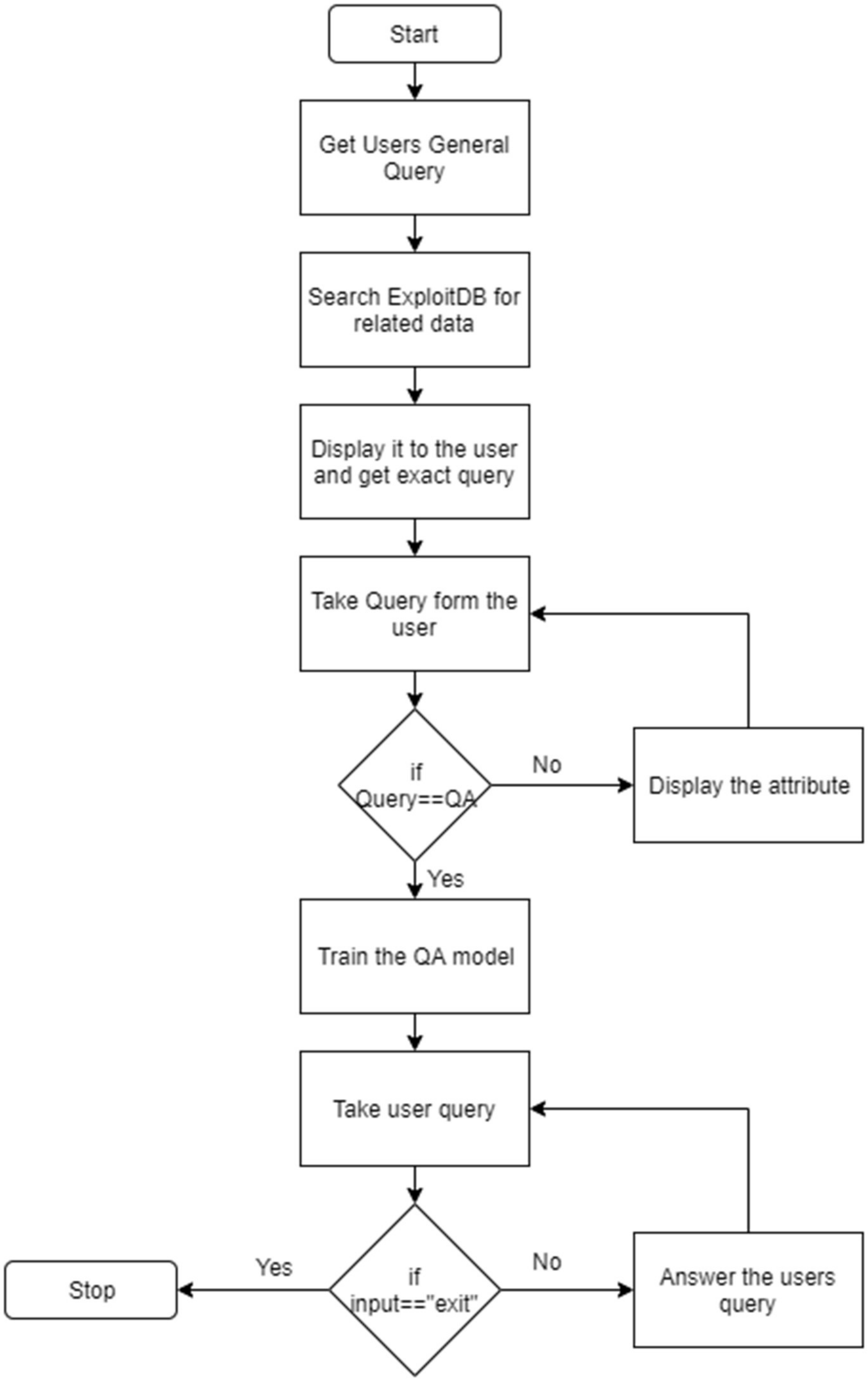
Due to these reasons the users face problems in communicating with the chatbots.

5.2 SCOPE

Due to high requirements and use of chat-bots on various kinds of services like customer service, personal assistance, and many more. With the development of this chat-bot users can easily get the key insights of huge data without going through the data himself. The user has to just give information about the vulnerability that he wants to find, once that's done the system gathers data using the National Vulnerability Database and trains on it to provide analysis and summarizations on the description provided by the NVD.

CHAPTER 6

PROPOSED SYSTEM



CHAPTER 7

METHODOLOGY

Domain adaptation is the process of teaching cognitive systems like Watson to understand the entities and relations that are used in a specific domain. The system developers and domain experts use the domain adaptation process to prepare the system to answer questions or provide information. In the current case, the domain is cyber security. Adaptation is an iterative process of experimentation, analysis, and development. The goal of the process is to tailor the system so that it can properly process the corpus of knowledge to provide relevant and meaningful information to the user. The system analyzes the linguistics of the question by decomposing the question using deep parsing and analyzing the question to understand what is being asked and what constraints are being imposed on the answer. Technologies like named entity recognizers (NERs) and name entity detectors (NEDs) pull out any recognized people, places, etc.; then using a slot grammar parser (XSG), Watson identifies parts of speech for some of terms, references, conferences, pronouns, detect relationships, etc. in the text. Lexical answer types (LATs) are determined in order to help form candidate answer searches and to score candidate answers by type match to the Focus of the query. Along with the full input text, derived inferences, Focus and LATs will be used to build potential queries in the next phase.

CHAPTER 8

ANALYSIS

We've discussed the various ways in which Watson is being trained to become a cognitive cyber security assistant. One can weave these threads together to illustrate more generally how a cognitive assistant should be trained using human expertise as Labeled Data for Supervised Learning. A human Cyber Security SME needs to: x Recognize cyber security terminology x Know how cyber security entities relate to each other x Be able to read, parse, and understand cyber security documents written by others x Know what questions to ask and where to go for the answers Notice that the several forms of training we have described in this paper are methods of capturing these forms of human understanding from the experts. Terminology is captured in the form of Dictionaries. Understanding of Entities and Relations is captured in the form of a Type System which is used by humans reading, parsing, and understanding documents via Human Annotation. Thousands of Question-Answer pairs collected from the cyber security SME's are used as the Ground Truth used to train the system to answer questions when assisting the next rising generation of Security Analysts. Last but not least, the iterative collection and curation of corpus content using feedback from users brings all of these steps together to refine the system's understanding of which content sources are trustworthy. We expect this system to improve greatly with time and iterative feedback through this process. Thus, the system becomes a Cyber Security expert advisor in order to assist humans in becoming experts in turn.

CHAPTER 9

HARDWARE AND SOFTWARE

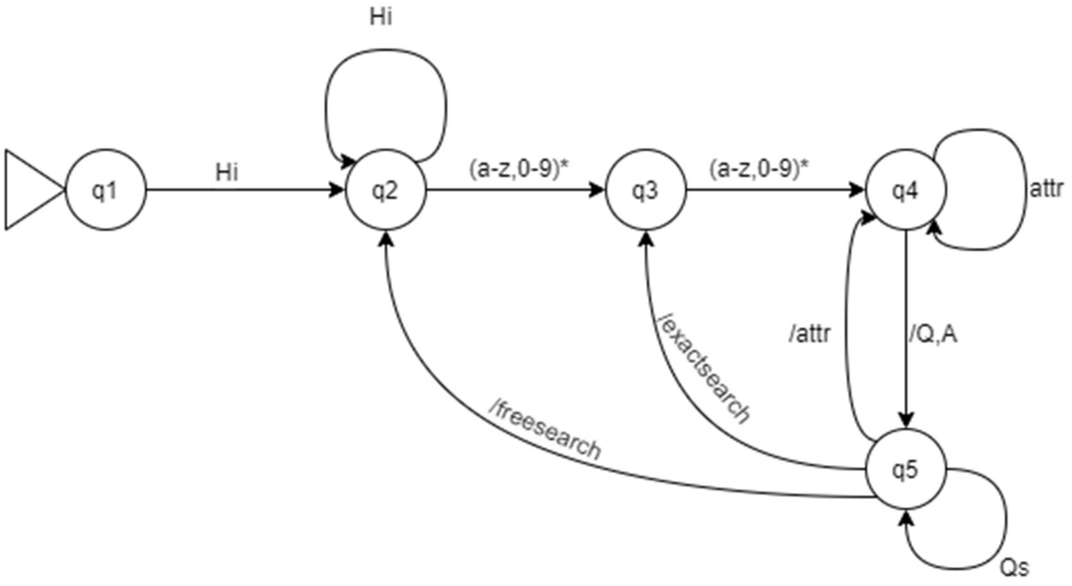
9.1 HARDWARE USED

Although there are replacements for each of the following devices but these were the one's chosen for demonstration, they are chosen taking into account their fitness in such an assembly. Abbreviations and Acronyms

9.1.1 A Computer

A computer with minimum specification is our only requirement in hardware. The laptop should be able to install and run the software like python, pytorch and BERT framework.

Fig (9.1.1). A Computer



9.2 SOFTWARES USED

9.2.1 Python

Python an interpreted, high-level, general-purpose programming language. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming.

Fig (9.2.1). Python

9.2.2 PyTorch

PyTorch is an open source machine learning library based on the Torch library, used for applications such as computer vision and natural language processing. PyTorch is composed of the following, Tensor library like NumPy with strong Graphics processing unit (GPU) support, a tape based automatic differentiation library that supports all differentiable Tensor operations in Torch, a neural networks library deeply integrated with Autograd which is designed for maximum flexibility.

Fig (9.2.2). PyTorch

9.2.3 BERT Framework

Google has recently open sourced a new technique for NLP pre-training called Bidirectional Encoder Representations from Transformers, or BERT. With this release, anyone in the world can train their own state-of-the-art question answering system (or a variety of other models) in about 30 minutes on a single Cloud TPU, or in a few hours using a single GPU.

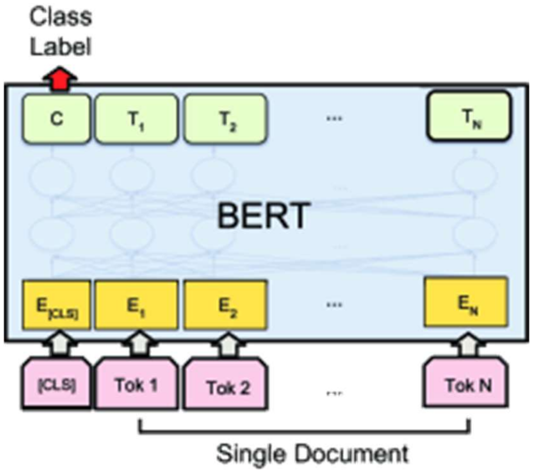
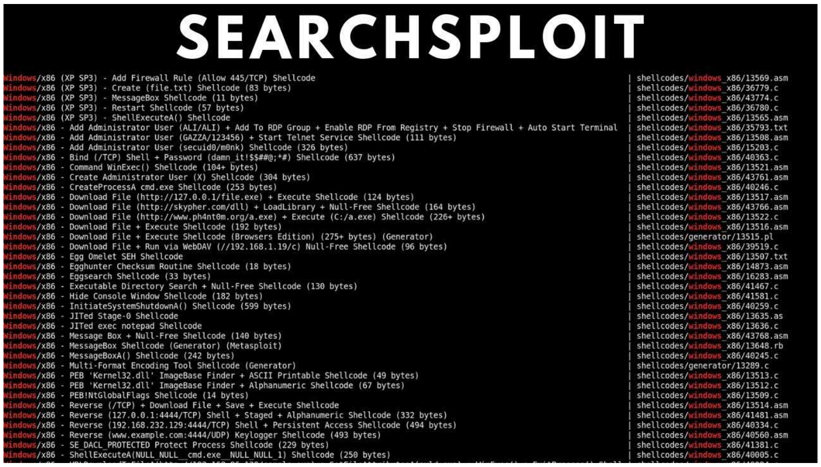


Fig (9.2.3). BERT Framework

9.2.4 Searchspliot

A command line search tool for Exploit-DB that also allows you to take a copy of Exploit Database with you, everywhere you go. SearchSploit gives you the power to perform detailed off-line searches through your locally checked-out copy of the repository. This capability is particularly useful for security assessments on segregated or air-gapped networks without Internet access.



SEARCHSPLOIT

```
Windows/x86 (XP SP3) - Add Firewall Rule (Allow 445/TCP) Shellcode                                                                 | shellcodes/windows_x86/13569.asm
Windows/x86 (XP SP3) - Create (file.txt) Shellcode (83 bytes)                                                                      | shellcodes/windows_x86/36779.c
Windows/x86 (XP SP3) - MessageBox Shellcode (11 bytes)                                                                             | shellcodes/windows_x86/43774.c
Windows/x86 (XP SP3) - Restart Shellcode (57 bytes)                                                                                | shellcodes/windows_x86/36780.c
Windows/x86 (XP SP3) - ShellExecuteA() Shellcode                                                                                   | shellcodes/windows_x86/13565.asm
Windows/x86 - Add Administrator User (ALI/ALI) + Add To RDP Group + Enable RDP From Registry + Stop Firewall + Auto Start Terminal | shellcodes/windows_x86/35793.txt
Windows/x86 - Add Administrator User (GAZZA/123456) + Start Telnet Service Shellcode (111 bytes)                                   | shellcodes/windows_x86/13508.asm
Windows/x86 - Add Administrator User (secuid0/m0nk) Shellcode (326 bytes)                                                          | shellcodes/windows_x86/15203.c
Windows/x86 - Bind (/TCP) Shell + Password (damn_it!$$##@;*#) Shellcode (637 bytes)                                                | shellcodes/windows_x86/40363.c
Windows/x86 - Command WinExec() Shellcode (104+ bytes)                                                                             | shellcodes/windows_x86/13521.asm
Windows/x86 - Create Administrator User (X) Shellcode (304 bytes)                                                                  | shellcodes/windows_x86/43761.asm
Windows/x86 - CreateProcessA cmd.exe Shellcode (253 bytes)                                                                         | shellcodes/windows_x86/40246.c
Windows/x86 - Download File (http://127.0.0.1/file.exe) + Execute Shellcode (124 bytes)                                            | shellcodes/windows_x86/13517.asm
Windows/x86 - Download File (http://skypher.com/dll) + LoadLibrary + Null-Free Shellcode (164 bytes)                               | shellcodes/windows_x86/43766.asm
Windows/x86 - Download File (http://www.ph4nt0m.org/a.exe) + Execute (C:/a.exe) Shellcode (226+ bytes)                             | shellcodes/windows_x86/13522.c
Windows/x86 - Download File + Execute Shellcode (192 bytes)                                                                        | shellcodes/windows_x86/13516.asm
Windows/x86 - Download File + Execute Shellcode (Browsers Edition) (275+ bytes) (Generator)                                        | shellcodes/generator/13515.pl
Windows/x86 - Download File + Run via WebDAV (//192.168.1.19/c) Null-Free Shellcode (96 bytes)                                     | shellcodes/windows_x86/39519.c
Windows/x86 - Egg Omelet SEH Shellcode                                                                                             | shellcodes/windows_x86/13507.txt
Windows/x86 - Egghunter Checksum Routine Shellcode (18 bytes)                                                                      | shellcodes/windows_x86/14873.asm
Windows/x86 - Eggsearch Shellcode (33 bytes)                                                                                       | shellcodes/windows_x86/16283.asm
Windows/x86 - Executable Directory Search + Null-Free Shellcode (130 bytes)                                                        | shellcodes/windows_x86/41467.c
Windows/x86 - Hide Console Window Shellcode (182 bytes)                                                                            | shellcodes/windows_x86/41581.c
Windows/x86 - InitiateSystemShutdownA() Shellcode (599 bytes)                                                                      | shellcodes/windows_x86/40259.c
Windows/x86 - JITed Stage-0 Shellcode                                                                                              | shellcodes/windows_x86/13635.as
Windows/x86 - JITed exec notepad Shellcode                                                                                         | shellcodes/windows_x86/13636.c
Windows/x86 - Message Box + Null-Free Shellcode (140 bytes)                                                                        | shellcodes/windows_x86/43768.asm
Windows/x86 - MessageBox Shellcode (Generator) (Metasploit)                                                                        | shellcodes/windows_x86/13648.rb
Windows/x86 - MessageBoxA() Shellcode (242 bytes)                                                                                  | shellcodes/windows_x86/40245.c
Windows/x86 - Multi-Format Encoding Tool Shellcode (Generator)                                                                     | shellcodes/generator/13289.c
Windows/x86 - PEB 'Kernel32.dll' ImageBase Finder + ASCII Printable Shellcode (49 bytes)                                           | shellcodes/windows_x86/13513.c
Windows/x86 - PEB 'Kernel32.dll' ImageBase Finder + Alphanumeric Shellcode (67 bytes)                                              | shellcodes/windows_x86/13512.c
Windows/x86 - PEB!NtGlobalFlags Shellcode (14 bytes)                                                                               | shellcodes/windows_x86/13509.c
Windows/x86 - Reverse (/TCP) + Download File + Save + Execute Shellcode                                                            | shellcodes/windows_x86/13514.asm
Windows/x86 - Reverse (127.0.0.1:4444/TCP) Shell + Staged + Alphanumeric Shellcode (332 bytes)                                     | shellcodes/windows_x86/41481.asm
Windows/x86 - Reverse (192.168.232.129:4444/TCP) Shell + Persistent Access Shellcode (494 bytes)                                   | shellcodes/windows_x86/40334.c
Windows/x86 - Reverse (www.example.com:4444/UDP) Keylogger Shellcode (493 bytes)                                                   | shellcodes/windows_x86/40560.asm
Windows/x86 - SE_DACL_PROTECTED Protect Process Shellcode (229 bytes)                                                              | shellcodes/windows_x86/41381.c
Windows/x86 - ShellExecuteA(NULL_NULL__cmd.exe__NULL_NULL_1) Shellcode (250 bytes)                                                 | shellcodes/windows_x86/40005.c
```

Fig (9.2.4). Searchspliot

9.2.5 JSON

JavaScript Object Notation is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types. It is a very common data format, with a diverse range of applications, such as serving as replacement for XML in AJAX systems.

9.2.6 Selenium

Selenium is a portable framework for testing web applications. Selenium provides a playback tool for authoring functional tests without the need to learn a test scripting language.

Fig (9.2.6). Selenium

9.2.7 Chrome Driver

WebDriver is an open source tool for automated testing of webapps across many browsers. It provides capabilities for navigating to web pages, user input, JavaScript execution, and more. ChromeDriver is a standalone server that implements the W3C WebDriver standard. ChromeDriver is available for Chrome on Android and Chrome on Desktop (Mac, Linux, Windows and ChromeOS).

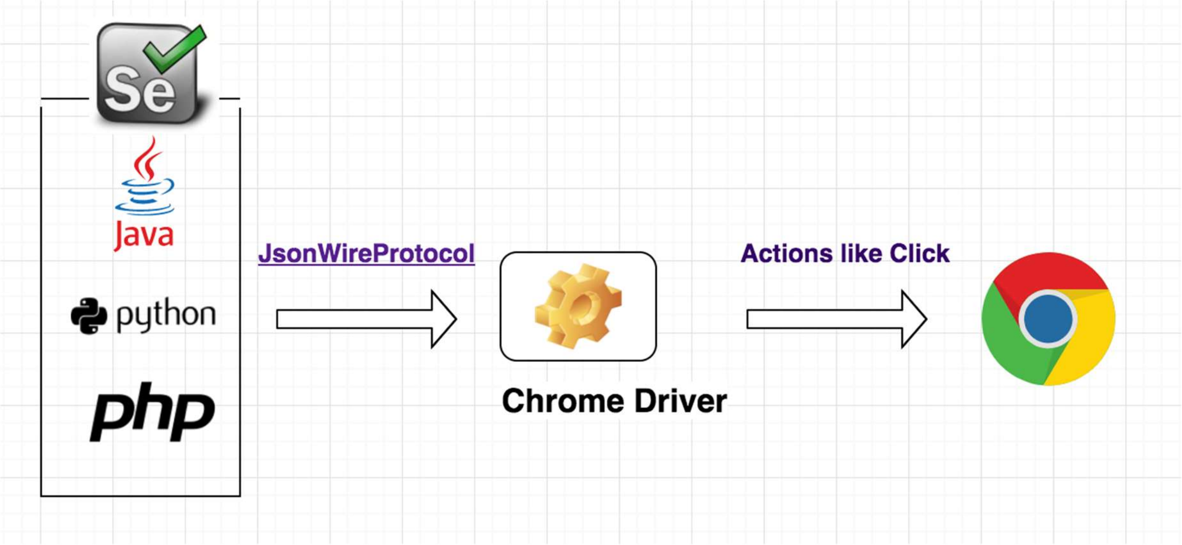


Fig (9.2.7). Chrome Driver

9.2.8 ExploitDB

The Exploit Database is an archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Its aim is to serve as the most comprehensive collection of exploits, shellcode and papers gathered through direct submissions, mailing lists, and other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and Proof-of-Concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

Fig (9.2.8). ExploitDB Logo

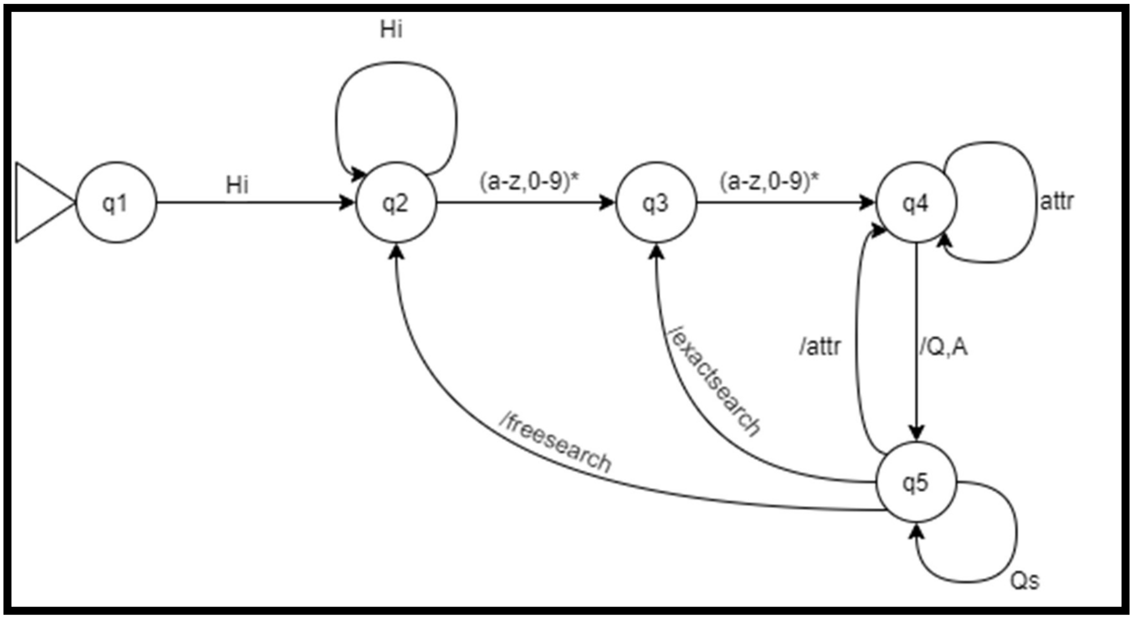
9.2.9 National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance.

Fig (9.2.9). NVD Logo

CHAPTER 10

DESIGN DETAILS

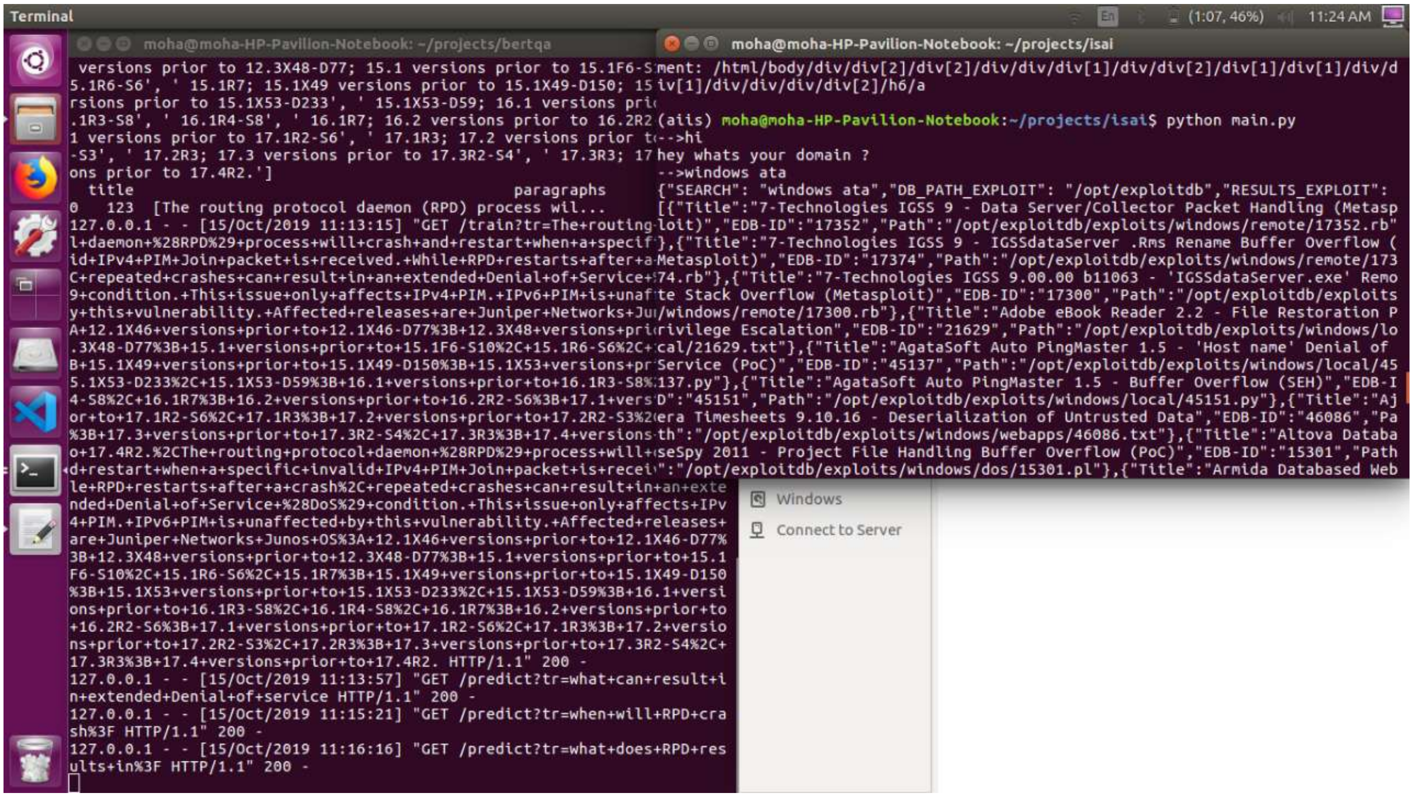


CHAPTER 11

IMPLEMENTATION PLAN

Main Functions:

To obtain report from user:

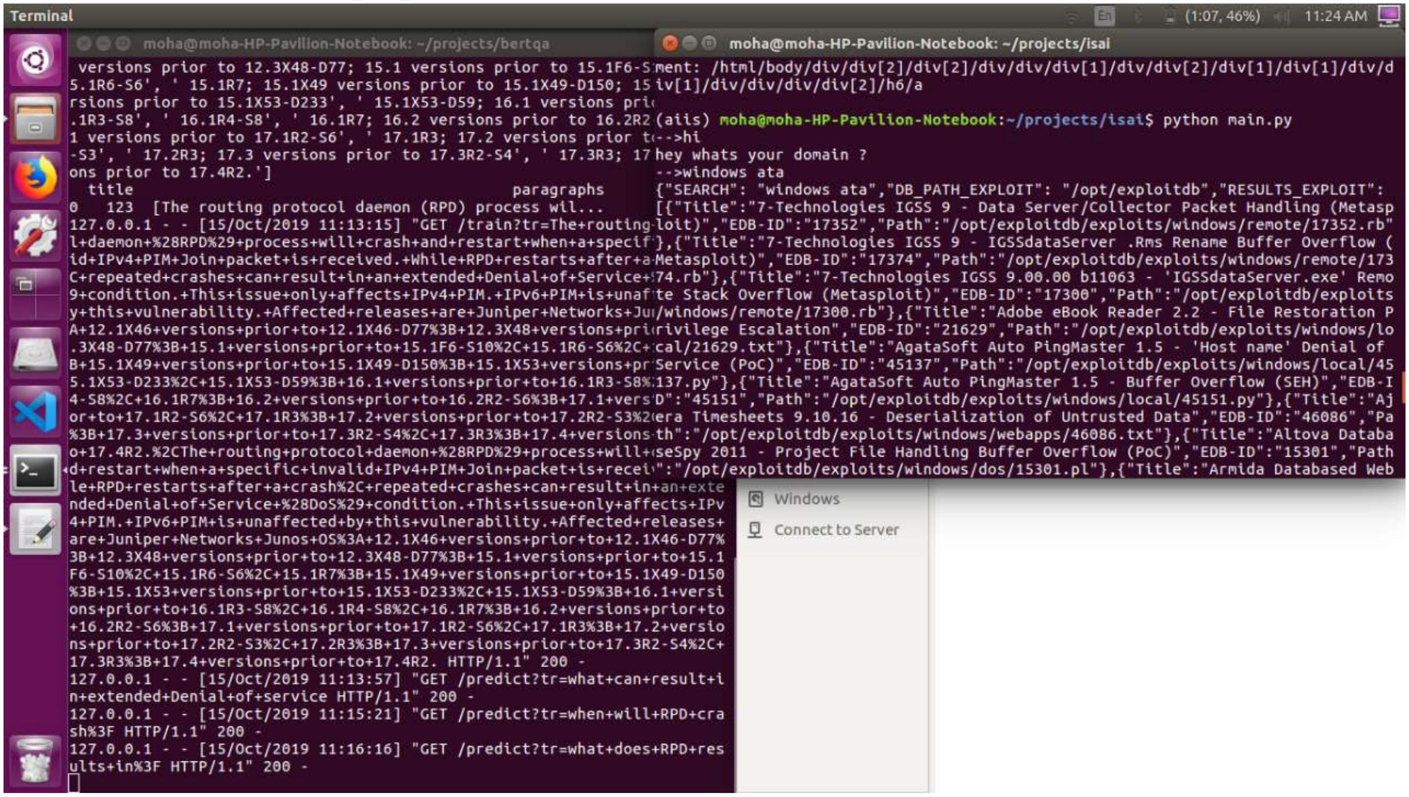

Terminal
(1:07, 46%)
11:24 AM
moha@moha-HP-Pavilion-Notebook: ~/projects/bertqa
moha@moha-HP-Pavilion-Notebook: ~/projects/isai
Windows
Connect to Server

```
 versions prior to 12.3X48-D77; 15.1 versions prior to 15.1F6-S
5.1R6-S6', ' 15.1R7; 15.1X49 versions prior to 15.1X49-D150; 15
rsions prior to 15.1X53-D233', ' 15.1X53-D59; 16.1 versions pri
.1R3-S8', ' 16.1R4-S8', ' 16.1R7; 16.2 versions prior to 16.2R2
1 versions prior to 17.1R2-S6', ' 17.1R3; 17.2 versions prior t
-S3', ' 17.2R3; 17.3 versions prior to 17.3R2-S4', ' 17.3R3; 17
ons prior to 17.4R2.']
  title                                            paragraphs
0   123  [The routing protocol daemon (RPD) process wil...
127.0.0.1 - - [15/Oct/2019 11:13:15] "GET /train?tr=The+routing
l+daemon+%28RPD%29+process+will+crash+and+restart+when+a+specif
id+IPv4+PIM+Join+packet+is+received.+While+RPD+restarts+after+a
C+repeated+crashes+can+result+in+an+extended+Denial+of+Service+
9+condition.+This+issue+only+affects+IPv4+PIM.+IPv6+PIM+is+unaf
y+this+vulnerability.+Affected+releases+are+Juniper+Networks+Ju
A+12.1X46+versions+prior+to+12.1X46-D77%3B+12.3X48+versions+pri
.3X48-D77%3B+15.1+versions+prior+to+15.1F6-S10%2C+15.1R6-S6%2C+
B+15.1X49+versions+prior+to+15.1X49-D150%3B+15.1X53+versions+pr
5.1X53-D233%2C+15.1X53-D59%3B+16.1+versions+prior+to+16.1R3-S8%
4-S8%2C+16.1R7%3B+16.2+versions+prior+to+16.2R2-S6%3B+17.1+vers
or+to+17.1R2-S6%2C+17.1R3%3B+17.2+versions+prior+to+17.2R2-S3%2
%3B+17.3+versions+prior+to+17.3R2-S4%2C+17.3R3%3B+17.4+versions
o+17.4R2.%2CThe+routing+protocol+daemon+%28RPD%29+process+will+
d+restart+when+a+specific+invalid+IPv4+PIM+Join+packet+is+recei
le+RPD+restarts+after+a+crash%2C+repeated+crashes+can+result+in+an+exte
nded+Denial+of+Service+%28DoS%29+condition.+This+issue+only+affects+IPv
4+PIM.+IPv6+PIM+is+unaffected+by+this+vulnerability.+Affected+releases+
are+Juniper+Networks+Junos+OS%3A+12.1X46+versions+prior+to+12.1X46-D77%
3B+12.3X48+versions+prior+to+12.3X48-D77%3B+15.1+versions+prior+to+15.1
F6-S10%2C+15.1R6-S6%2C+15.1R7%3B+15.1X49+versions+prior+to+15.1X49-D150
%3B+15.1X53+versions+prior+to+15.1X53-D233%2C+15.1X53-D59%3B+16.1+versi
ons+prior+to+16.1R3-S8%2C+16.1R4-S8%2C+16.1R7%3B+16.2+versions+prior+to
+16.2R2-S6%3B+17.1+versions+prior+to+17.1R2-S6%2C+17.1R3%3B+17.2+versio
ns+prior+to+17.2R2-S3%2C+17.2R3%3B+17.3+versions+prior+to+17.3R2-S4%2C+
17.3R3%3B+17.4+versions+prior+to+17.4R2. HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:13:57] "GET /predict?tr=what+can+result+i
n+extended+Denial+of+service HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:15:21] "GET /predict?tr=when+will+RPD+cra
sh%3F HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:16:16] "GET /predict?tr=what+does+RPD+res
ults+in%3F HTTP/1.1" 200 -
```

```
ment: /html/body/div/div[2]/div[2]/div/div/div[1]/div/div[2]/div[1]/div[1]/div/d
iv[1]/div/div/div/div[2]/h6/a

(aiis) moha@moha-HP-Pavilion-Notebook:~/projects/isai$ python main.py
-->hi
hey whats your domain ?
-->windows ata
{"SEARCH": "windows ata","DB_PATH_EXPLOIT": "/opt/exploitdb","RESULTS_EXPLOIT":
[{"Title":"7-Technologies IGSS 9 - Data Server/Collector Packet Handling (Metasp
loit)","EDB-ID":"17352","Path":"/opt/exploitdb/exploits/windows/remote/17352.rb"
},{"Title":"7-Technologies IGSS 9 - IGSSdataServer .Rms Rename Buffer Overflow (
Metasploit)","EDB-ID":"17374","Path":"/opt/exploitdb/exploits/windows/remote/173
74.rb"},{"Title":"7-Technologies IGSS 9.00.00 b11063 - 'IGSSdataServer.exe' Remo
te Stack Overflow (Metasploit)","EDB-ID":"17300","Path":"/opt/exploitdb/exploits
/windows/remote/17300.rb"},{"Title":"Adobe eBook Reader 2.2 - File Restoration P
rivilege Escalation","EDB-ID":"21629","Path":"/opt/exploitdb/exploits/windows/lo
cal/21629.txt"},{"Title":"AgataSoft Auto PingMaster 1.5 - 'Host name' Denial of
Service (PoC)","EDB-ID":"45137","Path":"/opt/exploitdb/exploits/windows/local/45
137.py"},{"Title":"AgataSoft Auto PingMaster 1.5 - Buffer Overflow (SEH)","EDB-I
D":"45151","Path":"/opt/exploitdb/exploits/windows/local/45151.py"},{"Title":"Aj
era Timesheets 9.10.16 - Deserialization of Untrusted Data","EDB-ID":"46086","Pa
th":"/opt/exploitdb/exploits/windows/webapps/46086.txt"},{"Title":"Altova Databa
seSpy 2011 - Project File Handling Buffer Overflow (PoC)","EDB-ID":"15301","Path
":"/opt/exploitdb/exploits/windows/dos/15301.pl"},{"Title":"Armida Databased Web
```

To train the model and prepare the chatbot for Q&A:


Terminal
(1:07, 46%)
11:24 AM
moha@moha-HP-Pavilion-Notebook: ~/projects/bertqa
moha@moha-HP-Pavilion-Notebook: ~/projects/isai
Windows
Connect to Server

```
 versions prior to 12.3X48-D77; 15.1 versions prior to 15.1F6-S
5.1R6-S6', ' 15.1R7; 15.1X49 versions prior to 15.1X49-D150; 15
rsions prior to 15.1X53-D233', ' 15.1X53-D59; 16.1 versions pri
.1R3-S8', ' 16.1R4-S8', ' 16.1R7; 16.2 versions prior to 16.2R2
1 versions prior to 17.1R2-S6', ' 17.1R3; 17.2 versions prior t
-S3', ' 17.2R3; 17.3 versions prior to 17.3R2-S4', ' 17.3R3; 17
ons prior to 17.4R2.']
  title                                          paragraphs
0   123  [The routing protocol daemon (RPD) process wil...
127.0.0.1 - - [15/Oct/2019 11:13:15] "GET /train?tr=The+routing
l+daemon+%28RPD%29+process+will+crash+and+restart+when+a+specif
id+IPv4+PIM+Join+packet+is+received.+While+RPD+restarts+after+a
C+repeated+crashes+can+result+in+an+extended+Denial+of+Service+
9+condition.+This+issue+only+affects+IPv4+PIM.+IPv6+PIM+is+unaf
y+this+vulnerability.+Affected+releases+are+Juniper+Networks+Ju
A+12.1X46+versions+prior+to+12.1X46-D77%3B+12.3X48+versions+pri
.3X48-D77%3B+15.1+versions+prior+to+15.1F6-S10%2C+15.1R6-S6%2C+
B+15.1X49+versions+prior+to+15.1X49-D150%3B+15.1X53+versions+pr
5.1X53-D233%2C+15.1X53-D59%3B+16.1+versions+prior+to+16.1R3-S8%
4-S8%2C+16.1R7%3B+16.2+versions+prior+to+16.2R2-S6%3B+17.1+vers
or+to+17.1R2-S6%2C+17.1R3%3B+17.2+versions+prior+to+17.2R2-S3%2
%3B+17.3+versions+prior+to+17.3R2-S4%2C+17.3R3%3B+17.4+versions
o+17.4R2.%2CThe+routing+protocol+daemon+%28RPD%29+process+will+
d+restart+when+a+specific+invalid+IPv4+PIM+Join+packet+is+recei
le+RPD+restarts+after+a+crash%2C+repeated+crashes+can+result+in+an+exte
nded+Denial+of+Service+%28DoS%29+condition.+This+issue+only+affects+IPv
4+PIM.+IPv6+PIM+is+unaffected+by+this+vulnerability.+Affected+releases+
are+Juniper+Networks+Junos+OS%3A+12.1X46+versions+prior+to+12.1X46-D77%
3B+12.3X48+versions+prior+to+12.3X48-D77%3B+15.1+versions+prior+to+15.1
F6-S10%2C+15.1R6-S6%2C+15.1R7%3B+15.1X49+versions+prior+to+15.1X49-D150
%3B+15.1X53+versions+prior+to+15.1X53-D233%2C+15.1X53-D59%3B+16.1+versi
ons+prior+to+16.1R3-S8%2C+16.1R4-S8%2C+16.1R7%3B+16.2+versions+prior+to
+16.2R2-S6%3B+17.1+versions+prior+to+17.1R2-S6%2C+17.1R3%3B+17.2+versio
ns+prior+to+17.2R2-S3%2C+17.2R3%3B+17.3+versions+prior+to+17.3R2-S4%2C+
17.3R3%3B+17.4+versions+prior+to+17.4R2. HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:13:57] "GET /predict?tr=what+can+result+i
n+extended+Denial+of+service HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:15:21] "GET /predict?tr=when+will+RPD+cra
sh%3F HTTP/1.1" 200 -
127.0.0.1 - - [15/Oct/2019 11:16:16] "GET /predict?tr=what+does+RPD+res
ults+in%3F HTTP/1.1" 200 -
```

```
ment: /html/body/div/div[2]/div[2]/div/div/div[1]/div/div[2]/div[1]/div[1]/div/d
iv[1]/div/div/div/div[2]/h6/a

(aiis) moha@moha-HP-Pavilion-Notebook:~/projects/isai$ python main.py
-->hi
hey whats your domain ?
-->windows ata
{"SEARCH": "windows ata","DB_PATH_EXPLOIT": "/opt/exploitdb","RESULTS_EXPLOIT":
[{"Title":"7-Technologies IGSS 9 - Data Server/Collector Packet Handling (Metasp
loit)","EDB-ID":"17352","Path":"/opt/exploitdb/exploits/windows/remote/17352.rb"
},{"Title":"7-Technologies IGSS 9 - IGSSdataServer .Rms Rename Buffer Overflow (
Metasploit)","EDB-ID":"17374","Path":"/opt/exploitdb/exploits/windows/remote/173
74.rb"},{"Title":"7-Technologies IGSS 9.00.00 b11063 - 'IGSSdataServer.exe' Remo
te Stack Overflow (Metasploit)","EDB-ID":"17300","Path":"/opt/exploitdb/exploits
/windows/remote/17300.rb"},{"Title":"Adobe eBook Reader 2.2 - File Restoration P
rivilege Escalation","EDB-ID":"21629","Path":"/opt/exploitdb/exploits/windows/lo
cal/21629.txt"},{"Title":"AgataSoft Auto PingMaster 1.5 - 'Host name' Denial of
Service (PoC)","EDB-ID":"45137","Path":"/opt/exploitdb/exploits/windows/local/45
137.py"},{"Title":"AgataSoft Auto PingMaster 1.5 - Buffer Overflow (SEH)","EDB-I
D":"45151","Path":"/opt/exploitdb/exploits/windows/local/45151.py"},{"Title":"Aj
era Timesheets 9.10.16 - Deserialization of Untrusted Data","EDB-ID":"46086","Pa
th":"/opt/exploitdb/exploits/windows/webapps/46086.txt"},{"Title":"Altova Databa
seSpy 2011 - Project File Handling Buffer Overflow (PoC)","EDB-ID":"15301","Path
":"/opt/exploitdb/exploits/windows/dos/15301.pl"},{"Title":"Armida Databased Web
```

Code Snippets:

```
from searchspl import searc
import json
from scr import CVE
from JsonSearch import dessearc
import requests

URLtr = "http://127.0.0.1:5000/train"
URLpr = "http://127.0.0.1:5000/predict"
state = "q1"
cve = 0
global attrlis

def q1(inp):
        if inp0 == 'hello' or 'hi' or 'hey' or 'sup' or 'wasup':
                global state
                state = 'q2'
                # print(state)
                #print("q1")
                return "hey whats your domain?"
        else:
                return "I wasn't able to understand please reframe"
                return attrlis. cvssv3_baseSeverity
        if inp == "cvssv3_exploitabilityScore":
                return attrlis. cvssv3_exploitabilityScore
        if inp == "cvssv3_impactScore":
                return attrlis. cvssv3_impactScore
        if inp == "cvssv2_accessComplexity":
```

```
        return attrlis. cvssv2_accessComplexity
    if inp == "cvssv2_authentication":
        return attrlis. cvssv2_authentication

def q5(inp):
    if inp == "bye":
        state = "q9"
        return "Bye"
    PARAMS = {'tr':inp}
    rr = requests.get(url = URLpr, params = PARAMS)
    return rr.content

while True:
    # global state
    inp0=input('-->')
    #print("sta ",state)
    if state == "q1":
        out0 = q1(inp0)
        print(out0)
    elif state == "q2":
        out0 = q2(inp0)
        print(out0)
    elif state == "q3":
        out0 = q3(inp0)
        print("enter what attribute you want, enter qa to enter qa mode")
    elif state == "q4":
        out0 = q4(inp0)
        print(out0)
```

```
elif state == "q5":
        out0 = q5(inp0)
        print(out0)
else:
        print("thanks and bbye")
```

REFERENCES

[1] https://www.sogeti.com/globalassets/common/reports/ai-in-cybersecurity_report_v05.pdf

[2] https://www.ibm.com/security/artificial-intelligence

[3] https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx

[4] Hoon G.K., Yong L.J., Yang G.K. (2020) Interfacing Chatbot with Data Retrieval and Analytics Queries for Decision Making. In: P. P. Abdul Majeed A., Mat-Jizat J., Hassan M., Taha Z., Choi H., Kim J. (eds) RITA 2018. Lecture Notes in Mechanical Engineering. Springer, Singapore.

[5] Sayan, Carla & Hariri, Salim & Ball, George. (2017). Cyber Security Assistant: Design Overview. 313-317. 10.1109/FAS-W.2017.165.

[6] C. M. Sayan, "An Intelligent Security Assistant for Cyber Security Operations," 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W), Tucson, AZ, 2017, pp. 375-376. doi: 10.1109/FAS-W.2017.179