Giving Wings to Thoughts
ESTD : 2007

St. PETER'S ENGINEERING COLLEGE

UGC - AUTONOMOUS

Affiliated to JNTUH, Approved by AICTE, Accredited by NAAC with "A" Grade, NBA Programe Accredited (EEE, CSE, ECE)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MINI PROJECT PRESENTATION A.Y 24-25

SECTION : 4th CSE B

BATCH : 16

	Name	Roll No.
1.	Kyasalla Aparna	21BK1A05A3
2.	Kota Sandeep	21BK1A0596
3.	Kanchoji Aditya	21BK1A0588

Mrs. Poonam Chanakya

PROJECT GUIDE

HOD CSE

MINI PROJECT TITLE:

Gain Access of Metaploitable OS using Port Enumeration

PROBLEM STATEMENT

- As cybersecurity threats become more sophisticated, systems are increasingly vulnerable to exploitation due to unaddressed security flaws. Existing defense mechanisms, such as firewalls and antivirus software, often struggle to detect advanced attack techniques, leaving critical gaps in system security.
- The challenge is to understand how attackers exploit these vulnerabilities and to test and improve defensive mechanisms to counteract them effectively. Traditional security measures are reactive, often detecting attacks after they've occurred, which leads to unnecessary damage.

PROPOSED SOLUTION

- To address this issue, our solution combines offensive and defensive strategies. By creating and delivering custom **payloads** using tools like **Metasploit**, **MSFvenom**, and **Shellter**, we simulate realistic attacks to exploit vulnerabilities. At the same time, we evaluate defensive systems such as **IDS/IPS** and **antivirus software** to detect and mitigate these attacks in real-time, thereby improving both system security and response mechanisms. This comprehensive approach provides a balanced way to identify weaknesses while strengthening defense protocols.

EXISTING SOLUTIONS VS PROPOSED SOLUTION

Existing Solutions:

Firewalls: Block unauthorized access but struggle against advanced attacks.

Antivirus Software: Effective against known threats but fails to detect sophisticated, obfuscated payloads.

IDS/IPS: Detect known attack patterns but can miss novel, evasion techniques.

Limitations:

Reactive detection based on known signatures.

Miss newer or more sophisticated attack methods.

Proposed Solution:

Offensive-Defensive Integration: Combines Metasploit, MSFvenom, and Shellter for payload creation, obfuscation, and delivery.

Active Testing: Simulates real-world attacks to test defenses like IDS/IPS and antivirus software in real-time.

Benefits:

Proactively identifies vulnerabilities.

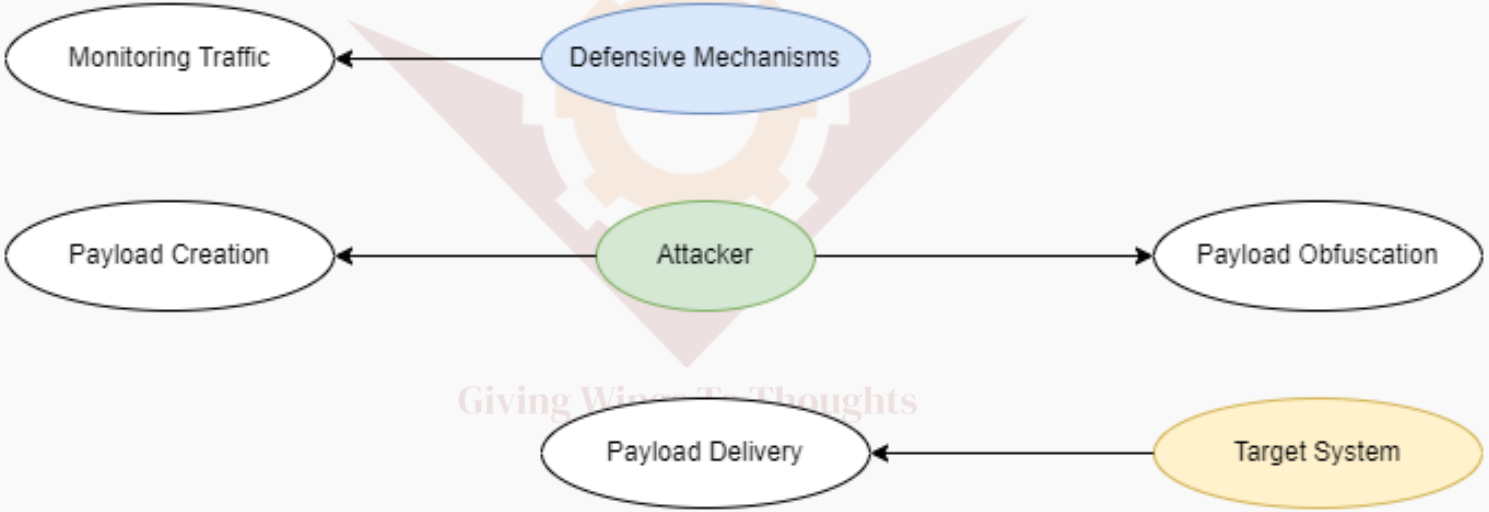
Improves defense systems by testing their ability to detect and block advanced attacks.

TECHNOLOGIES USED

1. **Metasploit Framework**: Used to manage and execute payloads, providing a comprehensive toolset for penetration testing and exploitation.
2. **MSFvenom**: Used to generate **custom payloads**, such as reverse TCP Meterpreter shells, that exploit vulnerabilities in the target system.
3. **Shellter**: A dynamic **payload obfuscation tool** to modify payloads and bypass **antivirus** detection, increasing the chances of a successful attack.
4. **Apache Server**: **Hosts the payload**, providing a platform to serve the malicious file to the target system over HTTP.
5. **IDS/IPS and Antivirus Software**: **Defensive tools** used to monitor and prevent malicious activities on the network. These systems help detect and mitigate attacks in real time.
6. **Windows 10**: The **target system** for simulating the attack. A typical modern OS used to test real-world exploit scenarios.

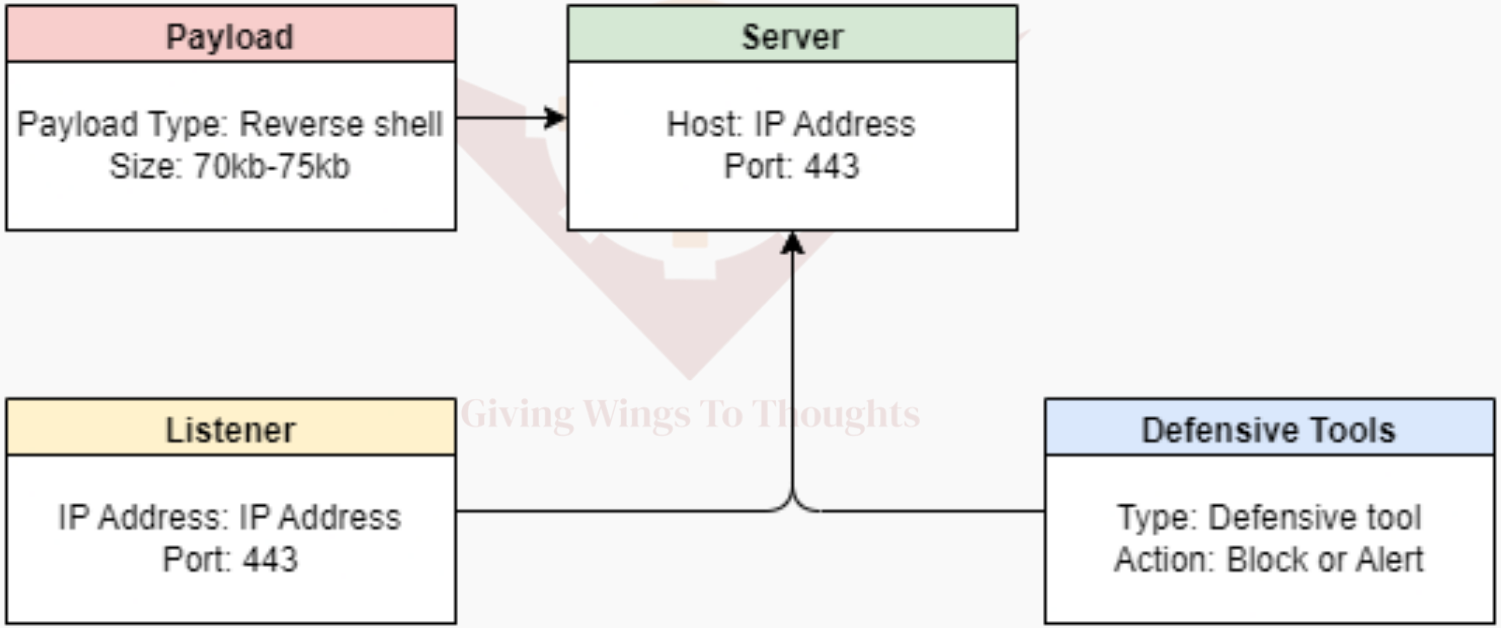
UML DIAGRAMS

USE-CASE DIAGRAM



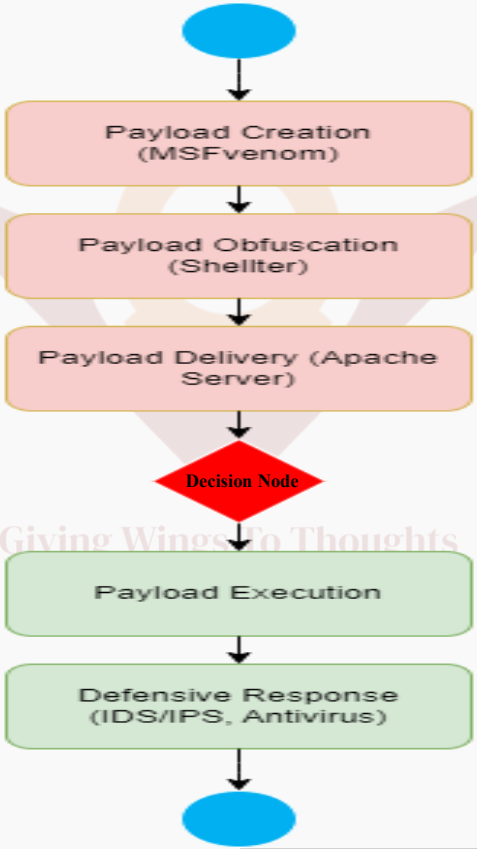
UML DIAGRAMS

CLASS DIAGRAM



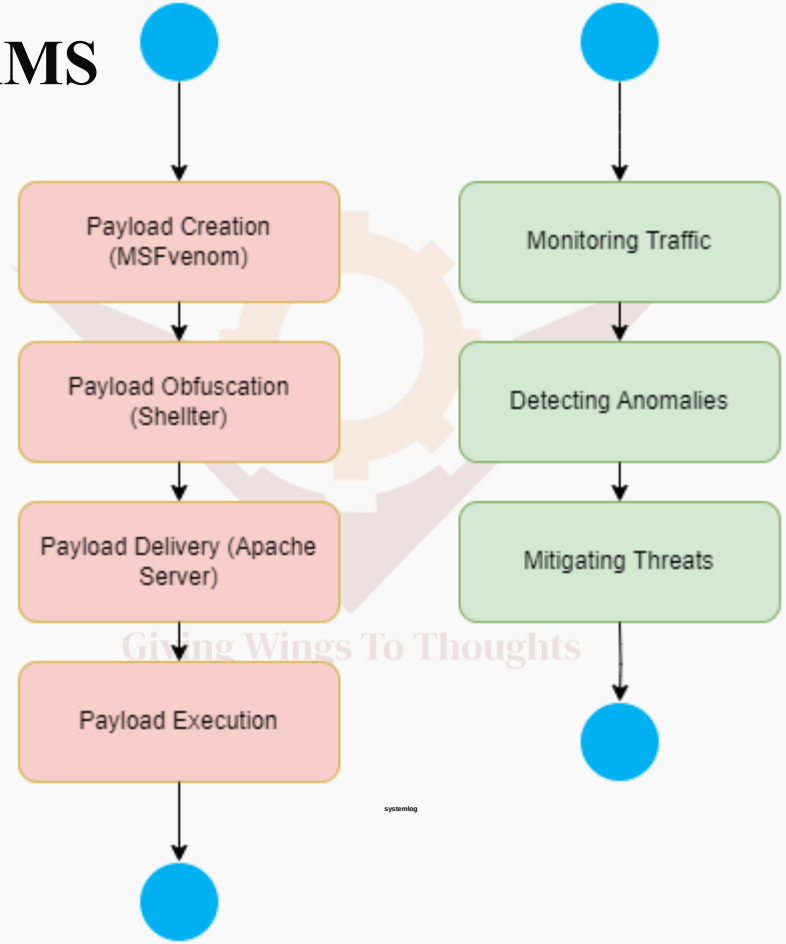
UML DIAGRAMS

ACTIVITY DIAGRAM

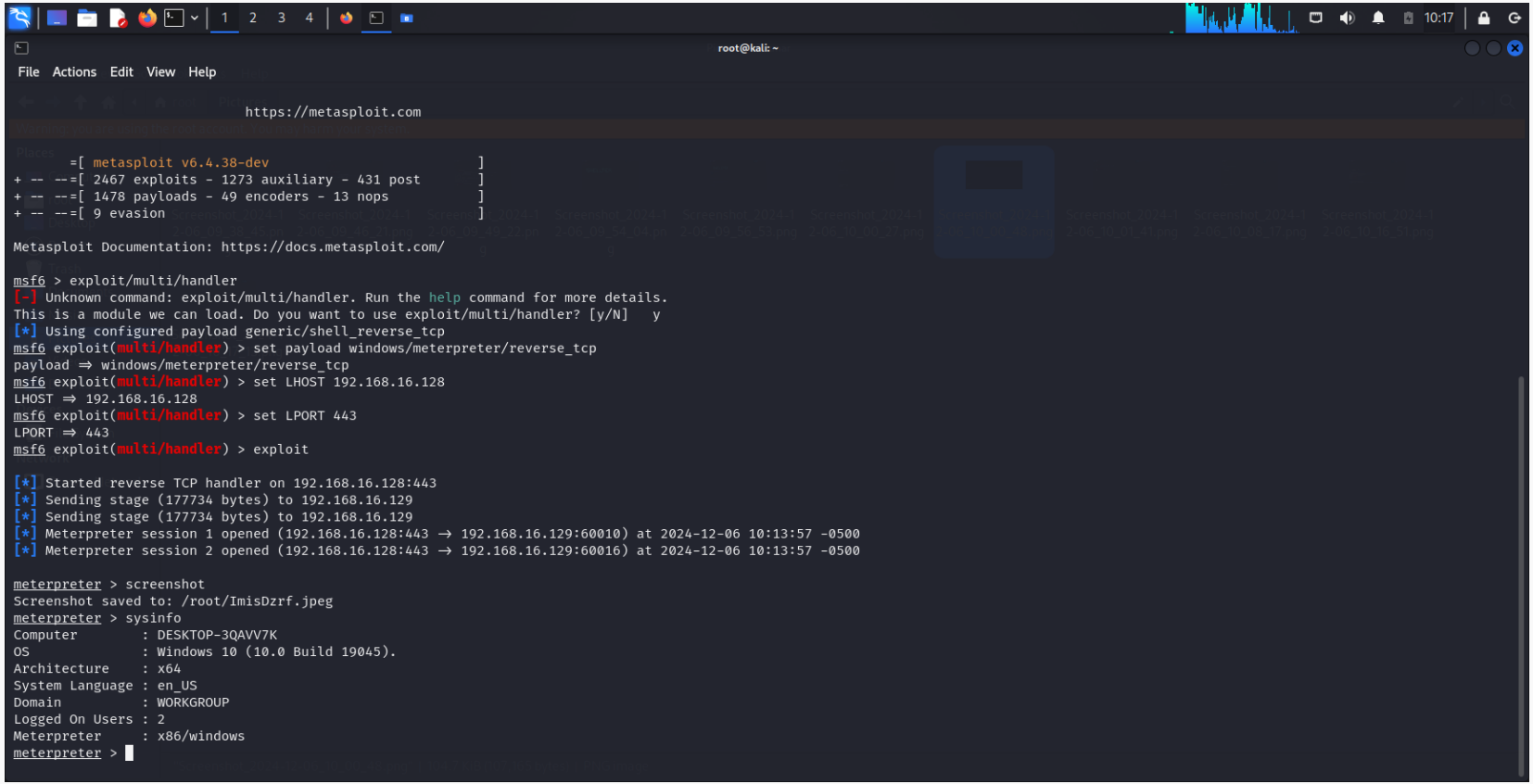


UML DIAGRAMS

SEQUENCE DIAGRAM



PROJECT OUTPUT



BENEFITS AND LIMITATIONS

Benefits:

- **Comprehensive Security Assessment**: Combines both **offensive techniques** (exploit creation and execution) and **defensive systems** (IDS/IPS, antivirus) to provide a holistic view of system security.
- **Proactive Defense Evaluation**: Simulates real-world attacks to test and strengthen existing security measures before an actual breach occurs.
- **Real-World Applicability**: Demonstrates how **payload obfuscation** can bypass traditional security systems and how **advanced detection tools** respond to evolving threats.
- **Improves Security Posture**: Identifies vulnerabilities in both the system and its defenses, leading to more robust defense strategies.

Limitations:

- **Testing Environment Constraints**: The project was tested in a controlled environment (Windows 10), and results may vary in more complex, real-world systems.
- **Firewall and Antivirus Evasion**: While obfuscation improved success, **firewalls** and **antivirus software** still prevented some payloads from executing.
- **Limited Defense Testing**: Focused on **IDS/IPS** and **antivirus**; other modern defense techniques, like **sandboxing**, were not tested.
- **Success Rate**: Only **50% success rate** in delivering the payload, indicating room for improvement in attack techniques.

CONCLUSION

•The project successfully demonstrated a **real-world attack simulation**, combining **offensive techniques** for exploiting vulnerabilities and **defensive mechanisms** to detect and mitigate these attacks.

•By using tools like **Metasploit**, **MSFvenom**, **Shellter**, and **Apache Server**, the project showcased how attackers can gain unauthorized access and how defensive systems can be tested for effectiveness.

•The project highlighted the **importance of integrating offensive and defensive strategies**, providing insights into the need for continuous improvement in cybersecurity defenses.

•While some challenges were faced, such as **firewall blocks** and **antivirus detection**, the project provided valuable lessons in improving **payload evasion techniques** and strengthening **network security**.

•Future work will focus on more advanced obfuscation, testing against **machine learning-based defenses**, and broader application to various systems.

PROJECT GUIDE

THANK YOU

- Batch 16

THANK YOU

- Batch 16

Giving Wings To Thoughts

Scan the QR for Further
Documentation and Research paper