Penetration Testing for Deerfield Beach Police Department

By

Cyber Security Intern Team

Aditi Rajesh Jadyal (C0904027)

Pratik Dhakal (C0917265)

Aadith Preetham (C0902681)

Opeyemi Alonge (C0901434)

Submission: **28 Mar 2025**

Table of Contents

Overview

This report provides a comprehensive penetration testing strategy conducted for the Deerfield Beach Police Department (DBPD) as part of a cybersecurity and digital forensics work-integrated learning project. The primary objective was to assess the effectiveness of Deerfield Beach Police Department's cybersecurity posture by simulating real-world attack scenarios in a controlled, ethical environment.

The report begins by explaining the importance of penetration testing in law enforcement settings, where the protection of sensitive data, systems, and infrastructure is paramount. It then outlines a step-by-step plan tailored to Deerfield Beach Police Department's operational environment, detailing each stage of the testing lifecycle—from reconnaissance to exploitation, privilege escalation, and reporting.

Three key attack methods were selected and executed in a virtual lab environment:

- Brute Force Attack
- Denial-of-Service (DoS) Attack
- Privilege Escalation

Each method is defined, demonstrated through screenshots, and analyzed for its value in identifying system weaknesses. Preventive strategies are also discussed to ensure real-world applicability.

The goal of this report is not only to identify technical vulnerabilities but to support Deerfield Beach Police Department's broader mission of ensuring public safety through secure digital operations. This document serves as a foundation for continuous cybersecurity improvements, awareness, and informed decision-making for future defense strategies.

Introduction

In today's digitally driven world, the threat landscape for cybercrime is evolving rapidly. Organizations, especially critical service providers like law enforcement agencies, are increasingly becoming high-value targets for malicious actors. Cyberattacks on police departments not only disrupt operations but can also compromise sensitive data, evidence systems, and public trust. In such a high-stakes environment, it is imperative for agencies like the Deerfield Beach Police Department (DBPD) to take a proactive and rigorous approach to securing their digital infrastructure.

One of the most effective ways to assess and improve the resilience of cybersecurity systems is through penetration testing, also known as ethical hacking. This method involves simulating real-world cyberattacks in a controlled and authorized environment to discover vulnerabilities before attackers do. Penetration testing does not just identify flaws; it also helps organizations understand the potential impact of those flaws and evaluate how well current defenses can detect and respond to threats.

For the Deerfield Beach Police Department, penetration testing is not only a cybersecurity best practice—it is a critical exercise in ensuring the confidentiality, integrity, and availability of law enforcement systems and data. It allows internal IT and security teams to validate their defenses against common attack vectors such as brute force, denial-of-service, and privilege escalation, which are widely used by cybercriminals and advanced persistent threats.

This report outlines a step-by-step penetration testing strategy tailored to Deerfield Beach Police Department's operational environment, supported by practical simulations conducted in a virtual lab. Additionally, it examines key attack methods used during the penetration test and provides both analysis and prevention strategies for each. The goal is to provide Deerfield Beach Police Department with actionable insights and a foundation for building a stronger, more secure digital infrastructure.

What is Penetration Testing and Why Is It Required for Cybersecurity System Evaluation?

Penetration Testing, also known as ethical hacking, is a structured process of simulating cyberattacks on an organization's digital infrastructure—such as networks, servers, applications, and endpoints—in order to identify and exploit potential vulnerabilities. The objective is to mimic the tactics and techniques that real-world attackers would use but in a controlled, authorized, and non-destructive manner. This allows security professionals to evaluate the strength of existing defenses, uncover weaknesses, and take corrective action before those flaws are exploited by malicious actors.

Unlike automated vulnerability scanners, penetration testing involves manual analysis, decision-making, and creativity—qualities that malicious hackers also employ. By thinking like an attacker, ethical hackers can gain a deeper understanding of how a system might be compromised and how much damage could be inflicted if it were breached.

Why Penetration Testing is Critical for Deerfield Beach Police Department

As a law enforcement agency, the Deerfield Beach Police Department (DBPD) manages a vast amount of sensitive data, including criminal records, investigative evidence, personnel details, and communication logs. A security breach could not only compromise ongoing investigations and sensitive intelligence but could also erode public trust and disrupt vital public safety operations. Penetration testing offers several critical benefits to Deerfield Beach Police Department:

1. Identifies Vulnerabilities Before Attackers Do

Penetration testing proactively uncovers weaknesses in systems, applications, or configurations that could be targeted by real attackers. This helps the department stay ahead of threats rather than reacting to incidents after damage has occurred.

2. Ensures Compliance with Legal and Regulatory Requirements

Many regulatory frameworks—such as CJIS (Criminal Justice Information Services), FISMA (Federal Information Security Management Act), and ISO/IEC 27001—require periodic security assessments. Penetration testing helps Deerfield Beach Police Department meet these compliance obligations and demonstrate due diligence in protecting sensitive law enforcement data.

3. Validates Security Controls and Incident Response Capabilities

A penetration test helps Deerfield Beach Police Department verify whether its firewalls, intrusion detection systems (IDS), access controls, and incident response mechanisms are functioning as intended. It evaluates the organization's ability to detect, respond to, and contain breaches in a timely manner.

4. Reduces the Risk of Data Breaches, Ransomware, and Downtime

Simulated attacks test the department's resilience to real-world threats such as ransomware, data exfiltration, and denial-of-service (DoS) attacks. Addressing the vulnerabilities identified in these tests helps reduce the likelihood of actual system compromises or service interruptions.

5. Supports a Culture of Continuous Cybersecurity Improvement

By identifying weaknesses and providing recommendations, penetration testing contributes to the ongoing refinement of Deerfield Beach Police Department's cybersecurity posture. It creates a feedback loop where lessons learned from tests are used to strengthen defenses, enhance policies, and guide future security investments.

Step-by-Step Plan to Use Penetration Testing for Deerfield Beach Police Department

1. Planning and Reconnaissance

- Define the scope of testing (IP range, systems involved).
- Identify rules of engagement and get authorization.
- Perform passive information gathering to learn about Deerfield Beach Police Department's systems.

2. Scanning and Enumeration

- Scan the network for live hosts, open ports, and running services.
- Enumerate user accounts, software versions, and vulnerabilities.

3. Gaining Access

- Exploit identified vulnerabilities to access Deerfield Beach Police Department systems.
- Use brute force, SQL injection, or other methods to gain initial entry.

4. Privilege Escalation and Lateral Movement

- Attempt to escalate privileges from a normal user to admin/root.
- Explore if access can be extended across systems.

5. Maintaining Access

- Simulate persistent backdoors (without causing harm).
- Mimic APT-style tactics to test long-term threat presence.

6. Reporting and Remediation Recommendations

- Document all findings with screenshots.
- Rate severity (Low, Medium, High).
- Suggest mitigation strategies and tools.

Penetration Testing Methods Used in This Plan

1. Brute Force Attack

Definition:
A brute force attack attempts to gain unauthorized access by trying multiple username-password combinations until the correct credentials are found.

Benefits in Exploitation:

- Identifies weak or reused passwords.
- Tests account lockout policies and user management.
- Highlights the lack of multi-factor authentication (MFA).

Prevention Measures:

- Use strong, complex passwords.
- Implement MFA.
- Set account lockout thresholds.

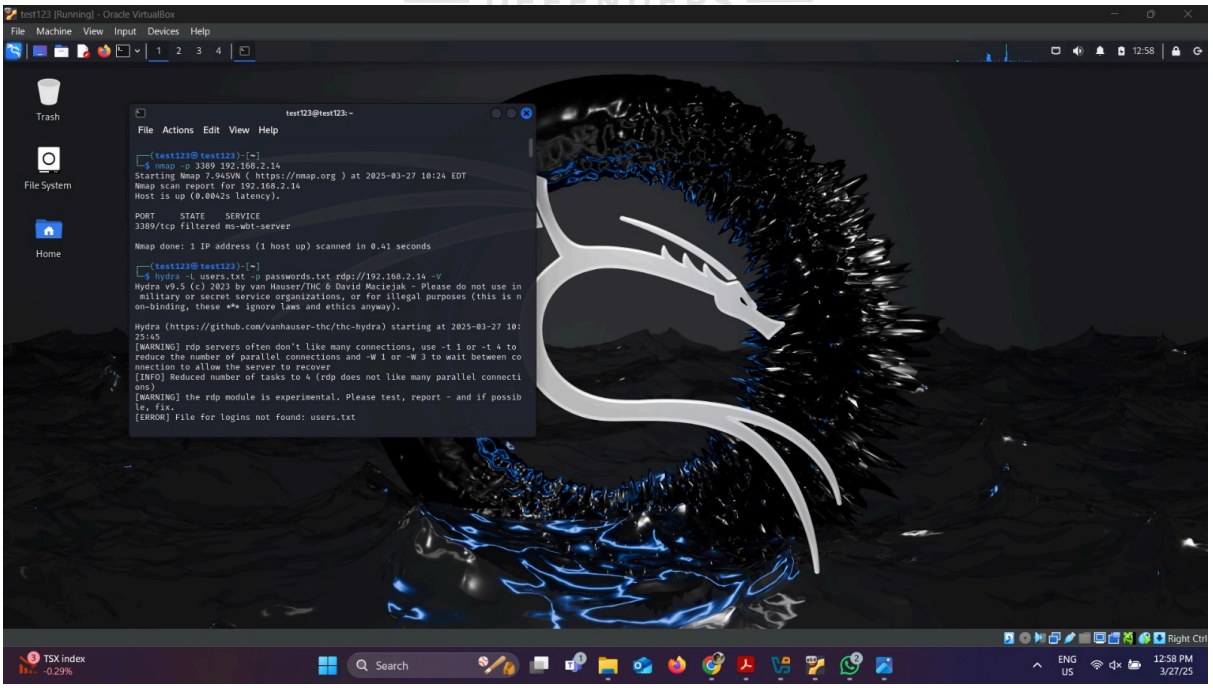

Fig 1: Scanning for vulnerability for bruteforce

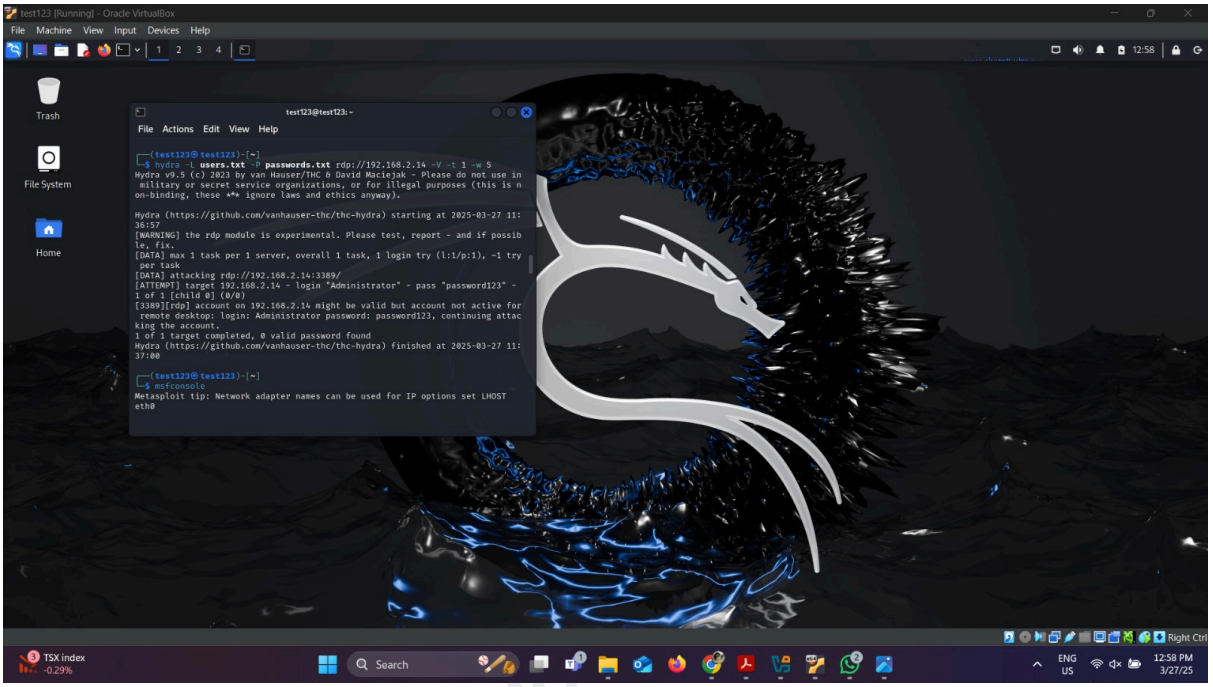

Fig 2: Brute Force Attack

2. Denial-of-Service (DoS) Attack

Definition:
A DoS attack aims to make a service or server unavailable by overwhelming it with traffic or resource exhaustion.

Benefits in Exploitation:

- Tests system resilience and availability.
- Identifies services that crash easily under load.
- Reveals poor network segmentation or firewall rules.

Prevention Measures:

- Use rate limiting and firewalls.
- Implement load balancing.
- Deploy DoS/DDoS protection services.

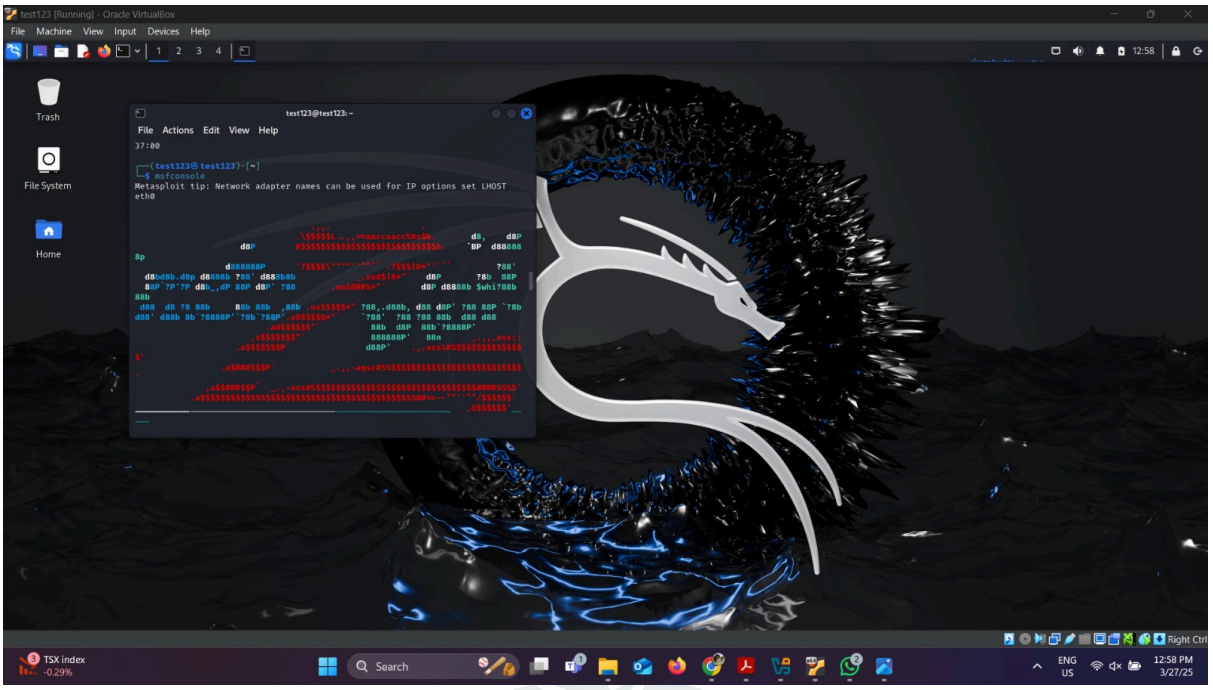

Fig 3: Using Metasploit for ddos

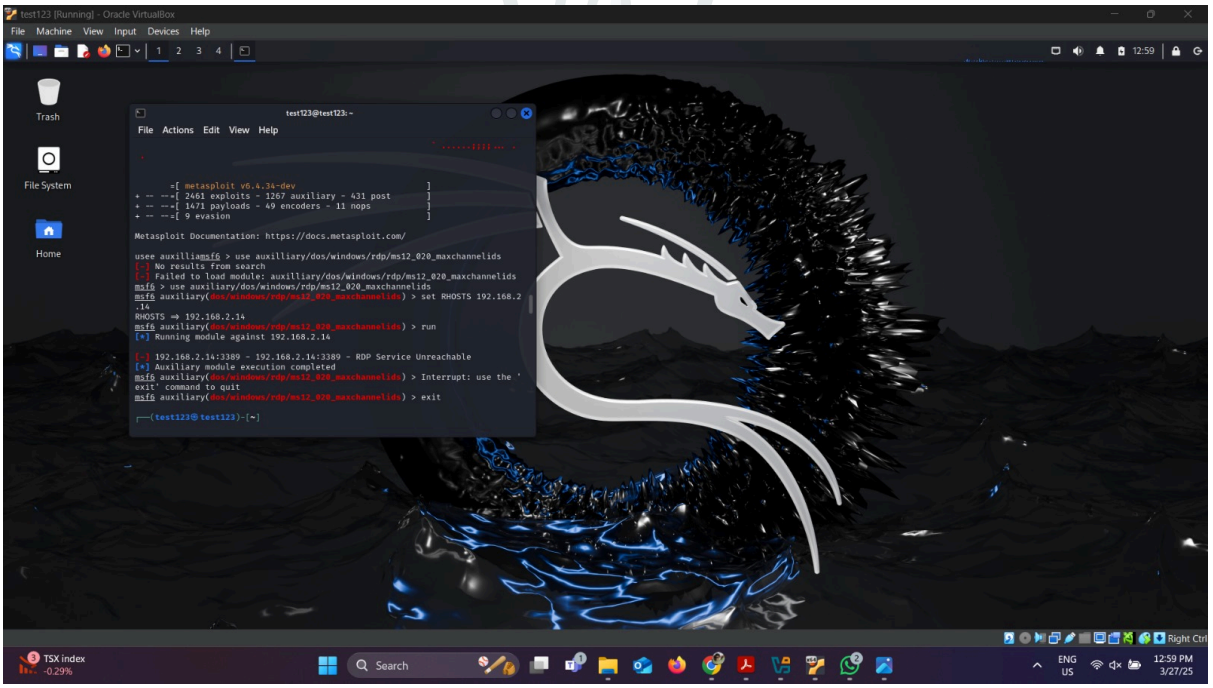

Fig 4: DdoS attack

3. Privilege Escalation

Definition:
This involves exploiting flaws or misconfigurations to move from a low-level account to one with administrative or root access.

Benefits in Exploitation:

- Exposes insecure system configurations.
- Tests the effectiveness of access controls and auditing.
- Simulates real attacker behavior post-initial compromise.

Prevention Measures:

- Regularly patch OS and software.
- Apply the principle of least privilege.
- Monitor user activity and permissions.

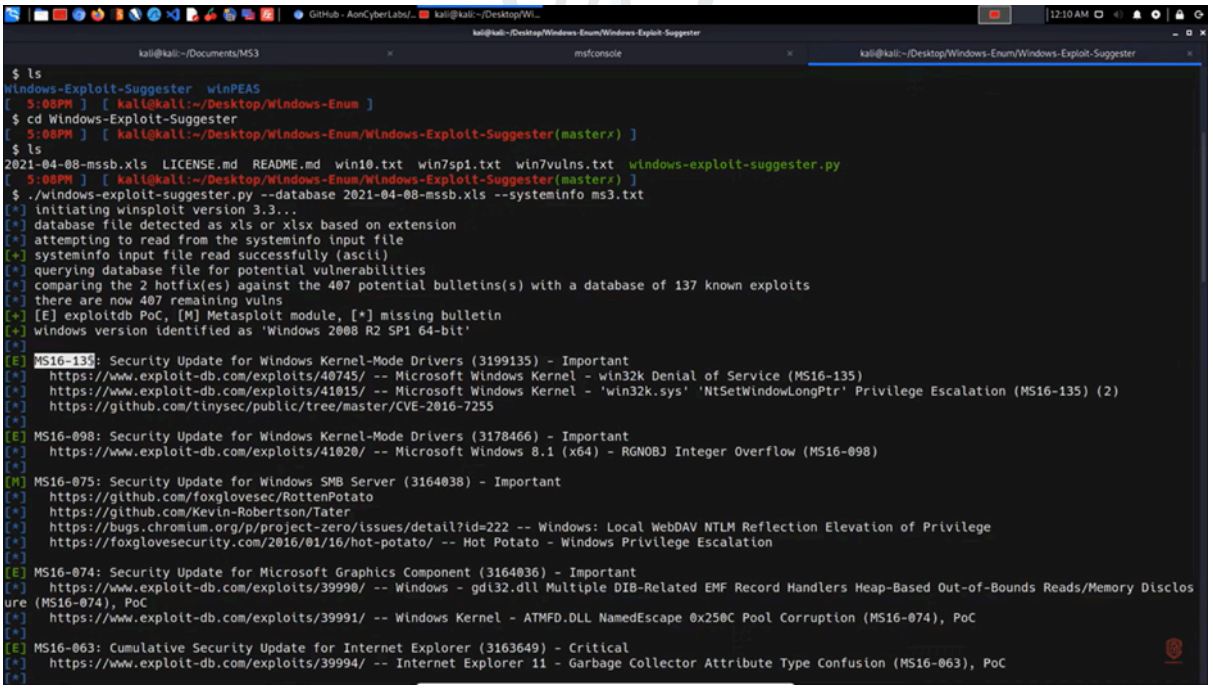

Fig 5: System information gathered from the target machine

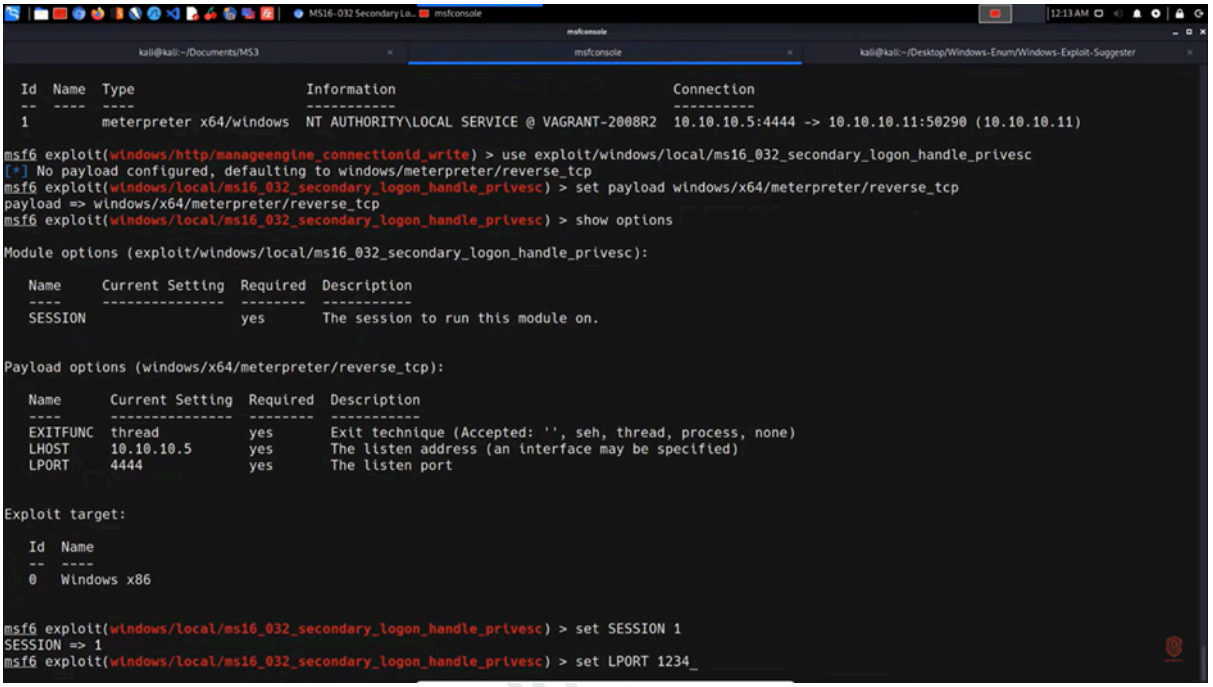

Fig 6: List of available exploits for the identified Windows system.

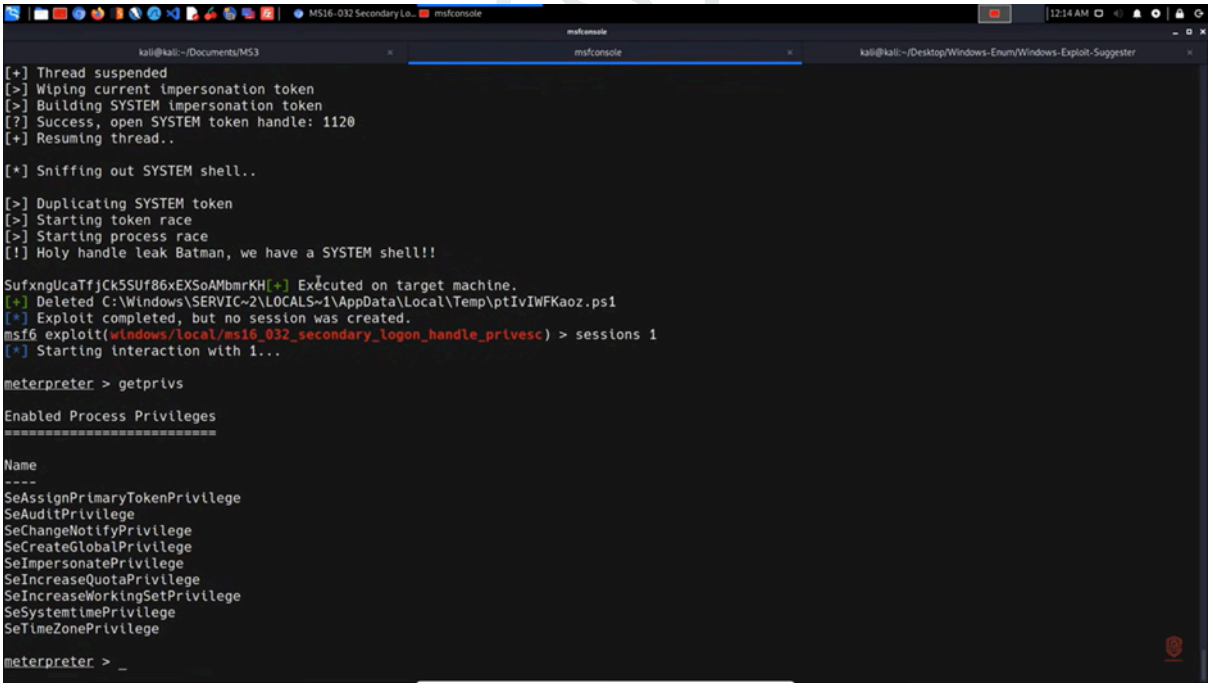

Fig 7: Exploit launched using Metasploit.

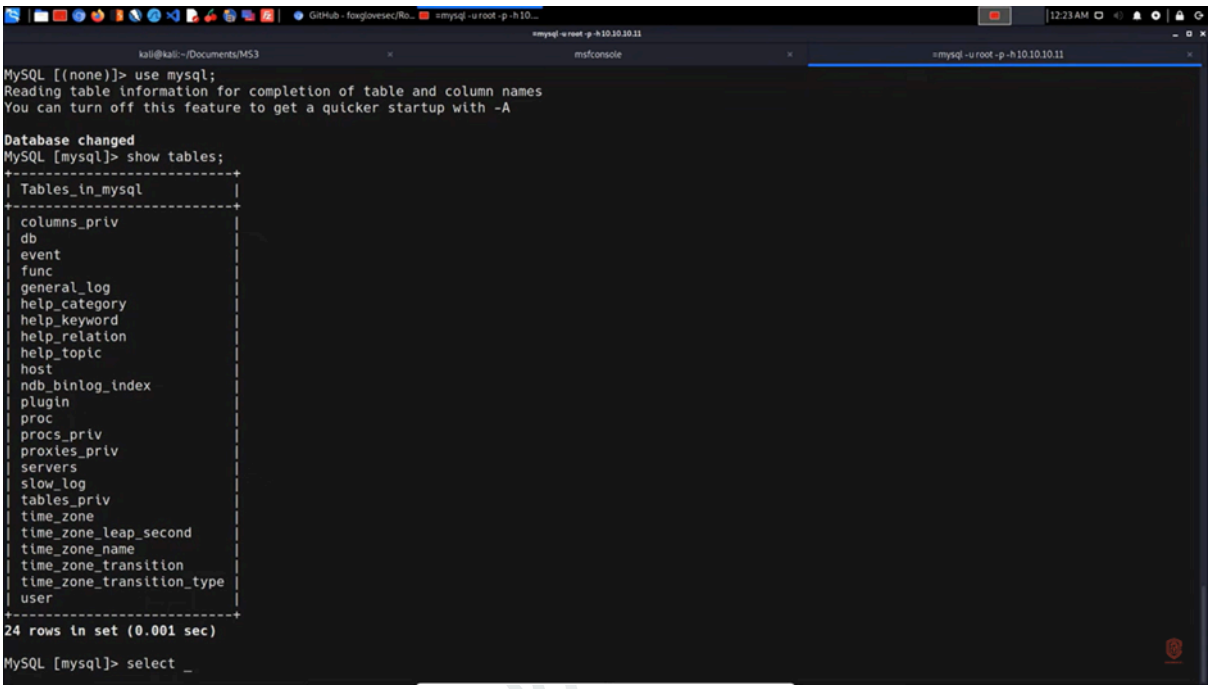

Fig 8: Attempting to list and impersonate tokens

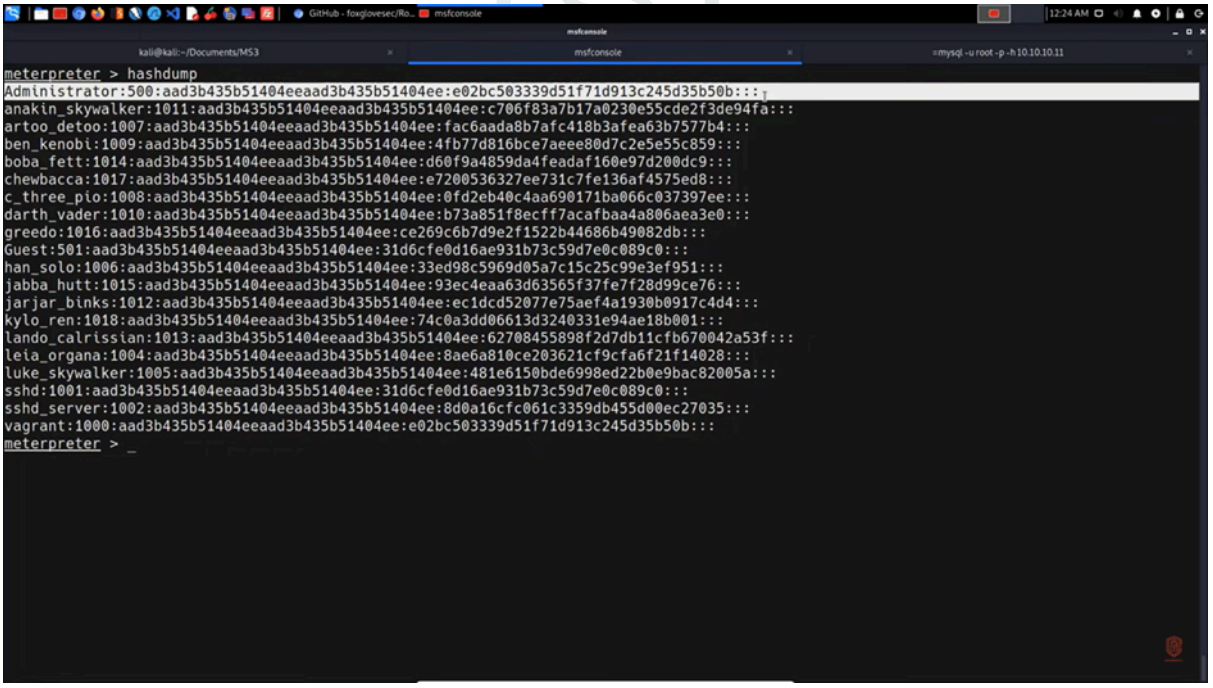

Fig 9: Privilege escalation using RottenPotato attack

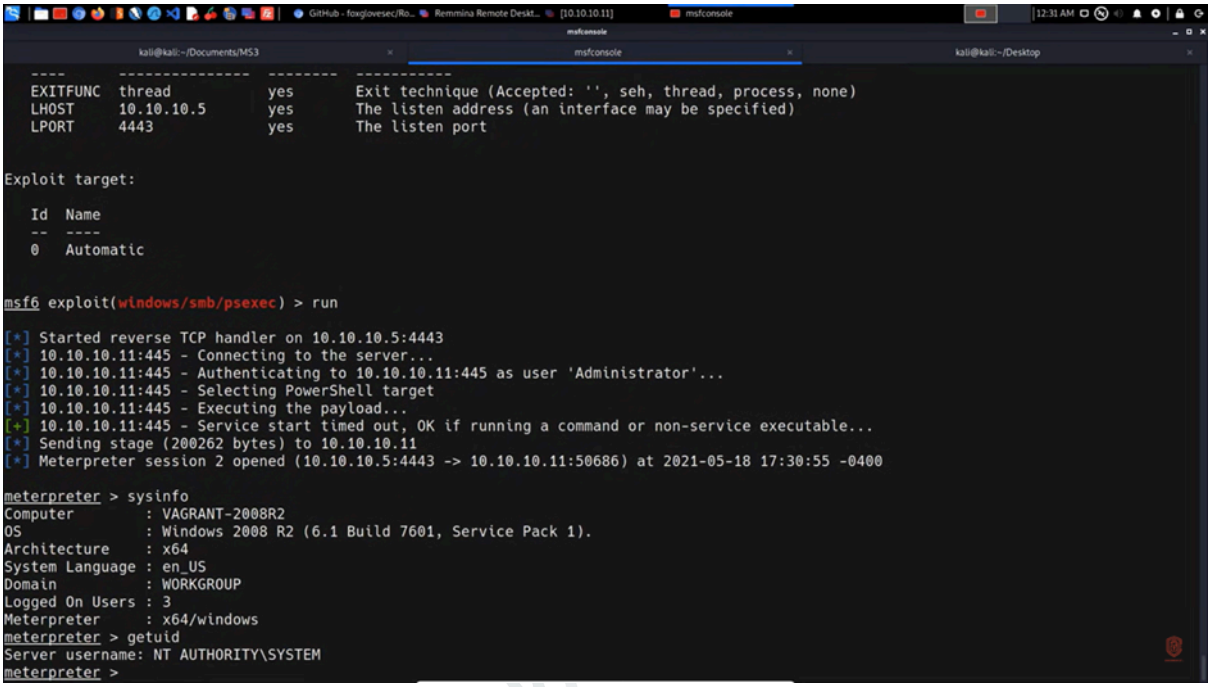

Fig 11: Access to administrator directory confirming SYSTEM privileges.

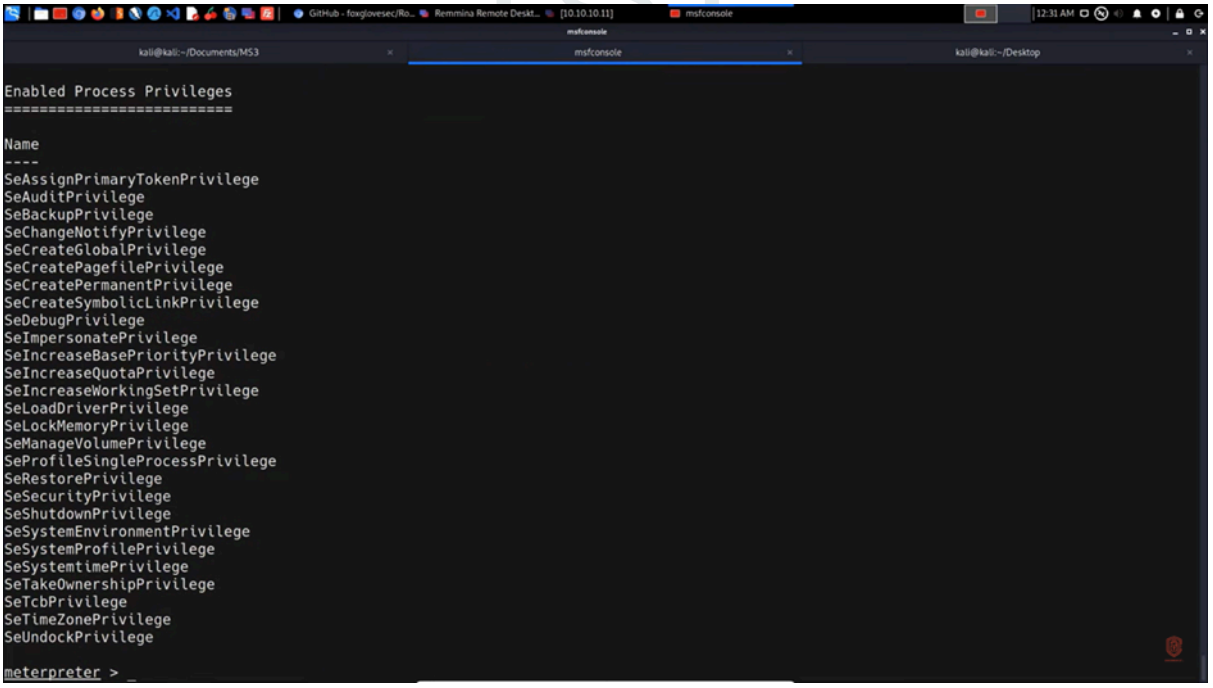

Fig 12: Access to administrator directory confirming SYSTEM privileges.

Conclusion

Penetration testing serves as a crucial line of defense for the Deerfield Beach Police Department (DBPD), offering a proactive strategy to uncover and address potential vulnerabilities. By simulating real-world attack scenarios such as brute force, denial-of-service, and privilege escalation, the department gains valuable insights into the effectiveness of its current security measures.

The findings from this exercise not only enhance the technical understanding of existing threats but also provide a foundation for implementing stronger access controls, incident response protocols, and ongoing training for staff. Moreover, these insights can inform future cybersecurity policies, budget planning for security tools, and continuous monitoring strategies to ensure long-term resilience.

References

- Access Token Manipulation, Technique T1134 - Enterprise | MITRE ATT&CK®. (n.d.). Retrieved from attack.mitre.org website: https://attack.mitre.org/techniques/T1134/
- Automated DDoS Mitigation. (2025, March). Retrieved March 28, 2025, from Cisco website: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-ddos-attack.html
- Chowdappa, K., Lakshmi, S., & Pavan Kumar, P. (n.d.). *Ethical Hacking Techniques with Penetration Testing*. Retrieved from https://www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.pdf
- Kaspersky. (2019). Brute force attack: Definition and examples. Retrieved from Kaspersky.com website: https://www.kaspersky.com/resource-center/definitions/brute-force-attack
- PTES. (2012, April 30). PTES Technical Guidelines - The Penetration Testing Execution Standard. Retrieved from Pentest-standard.org website: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*. NIST. Retrieved from NIST website: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- WSTG - v4.1 | OWASP Foundation. (2025). Retrieved March 28, 2025, from Owasp.org website: https://owasp.org/www-project-web-security-testing-guide/v41/2-Introduction/README.html

Time Sheet

Date	Task	Resource Name	Hours spent
March 21, 2025	Set up meeting to discuss the initial project scope	Pratik Dhakal Aditi Jadyal Aadith Preetham Opeyemi Alonge	6
March 23, 2025	Research on Penetration Testing and attack methods	Pratik Dhakal Opeyemi Alonge	10
March 25, 2025	Finding relevant cases and technical papers	Aditi Jadyal Aadith Preetham	3
March 25, 2025	Performing the attacks for practical testing	Aadith Preetham	6
March 27, 2025	Putting documentation and structure in the report	Pratik Dhakal, Aadith Preetham Aditi Jadyal	6
March 28, 2025	Finalisation, Submission and review from staff	Aadith Preetham	1
	Total Hours		**32 Hours**