Document Reference:	DTRTU-1	Effective Date:	29 April 2024
Document Name:	Data Theft Red Team Usecases	Expiry Date:	29 April 2024

Data Theft Red Team Usecases

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Liya Thomas
Next Review Date:	17 June 2024	Last Modified on:	19 April 2024

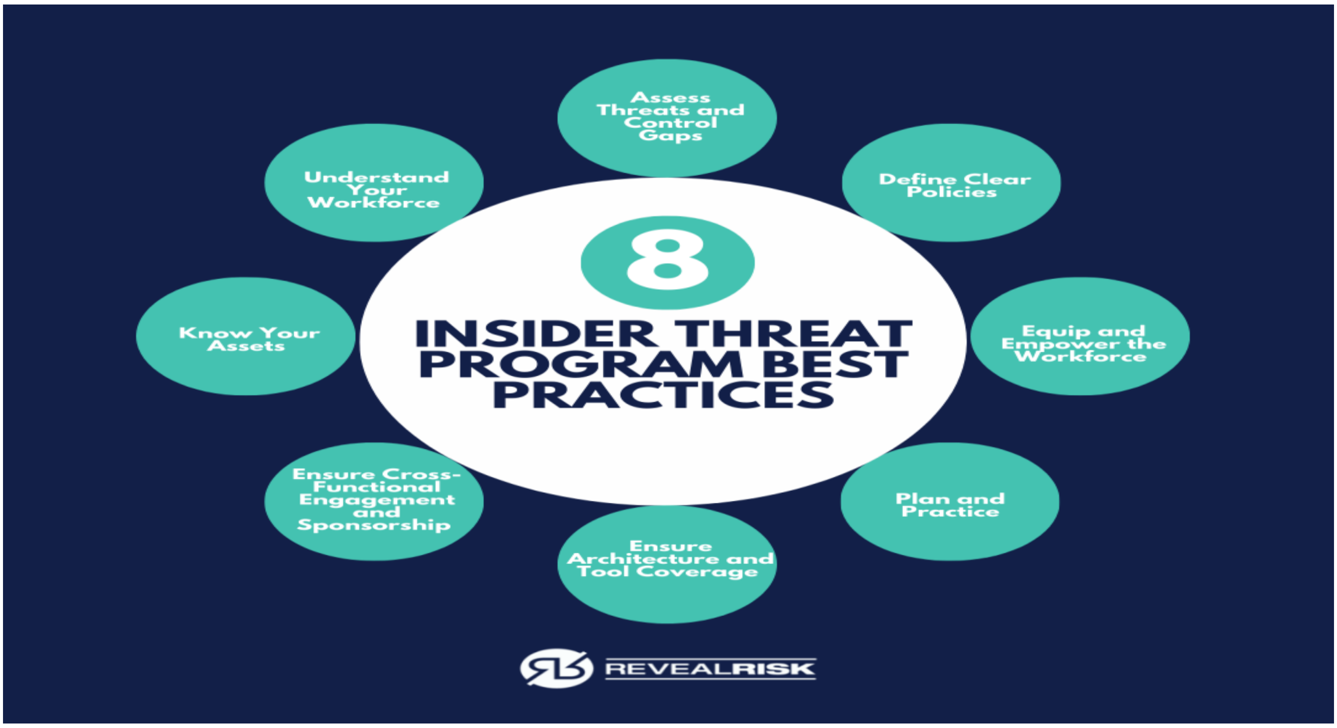
Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		19 April 2024	First Draft
0.2	Joel Daniel		29 April 2024	Cosmetic changes
1.0	Liya Thomas	Joel Daniel	29 April 2024	Approved for Publishing.

Table of Contents

1 Introduction:

Data theft is a big concern for companies. It can damage their reputation, finances, and compliance with regulations. The Red Team playbook for Data Theft Incident Response helps organizations prepare for such threats. It simulates different attack scenarios to see how well a company can detect, respond to, and minimize the impact of data theft incidents. This playbook gives a step-by-step guide for Red Team operations. It covers common ways attackers try to steal sensitive information, so companies can better defend against them.

2 Insider Threat:


8
INSIDER THREAT PROGRAM BEST PRACTICES
Assess Threats and Control Gaps
Define Clear Policies
Equip and Empower the Workforce
Plan and Practice
Ensure Architecture and Tool Coverage
Ensure Cross-Functional Engagement and Sponsorship
Know Your Assets
Understand Your Workforce
REVEALRISK

2.1 Objective:

Gain unauthorized access to sensitive data using an employee's credentials.

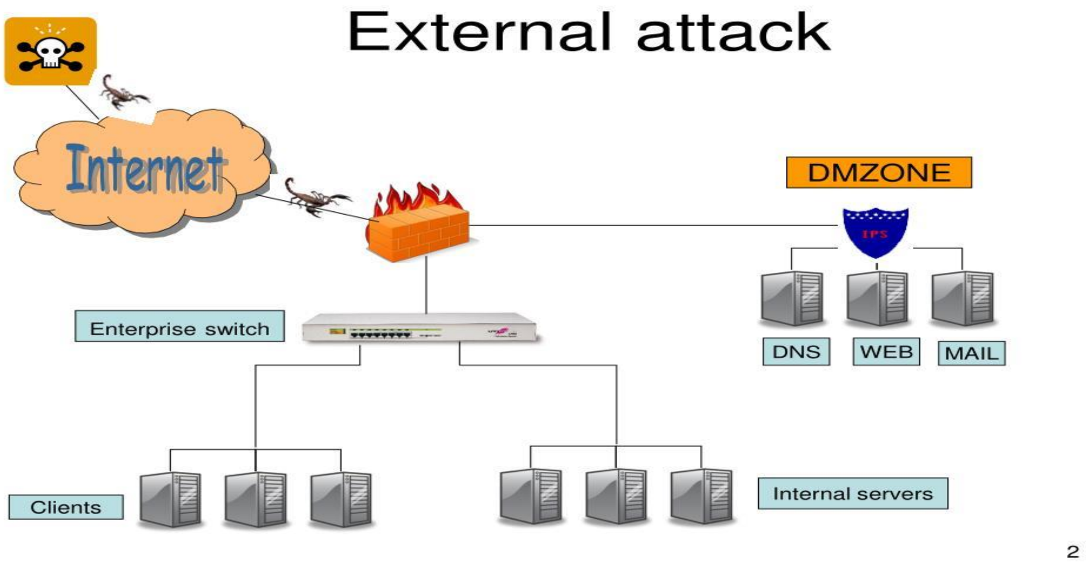
2.2 Steps:

1. Conduct reconnaissance to identify potential targets and their access levels: In this step, the attacker gathers information about employees within the organization, their roles, and their access privileges. They might use publicly available information, social media profiles, or even engage in physical surveillance to learn about potential targets and their access to sensitive data.
2. Phish target employee to obtain credentials or exploit existing vulnerabilities in their system: Phishing involves sending deceptive emails or messages to the target employee, tricking them into revealing their login credentials or downloading malicious software. The attacker may create convincing emails that appear to be from trusted sources, prompting the employee to click on links or enter sensitive information.
3. Use obtained credentials to access sensitive data: With the stolen credentials, the attacker gains access to the organization's systems or network. They navigate through the network using the compromised credentials, seeking out sensitive data such as customer information, financial records, or intellectual property.

2.3 Tools and Techniques:

- Social engineering: Social engineering techniques manipulate individuals into divulging confidential information or performing actions that compromise security. This can include tactics like pretexting (creating a fabricated scenario to gain trust), baiting (enticing targets with something appealing), or tailgating (following an authorized person to gain physical access).
- Phishing emails: Phishing emails are crafted to appear legitimate and deceive recipients into providing sensitive information or clicking on malicious links. Attackers often use psychological tactics to create a sense of urgency or importance, leading the recipient to act without thinking critically about the email's authenticity.
- Password cracking tools: Password cracking tools are software programs designed to guess or crack passwords used to secure accounts or systems. These tools utilize various techniques such as brute force attacks (trying all possible combinations) or dictionary attacks (trying common words or phrases) to break into accounts with weak or easily guessable passwords.

3 External Attack:



3.1 Objective:

Gain access to the company's network and exfiltrate sensitive data.

3.2 Steps:

1. Scan the company's network for vulnerabilities: In this step, the attacker uses specialized software known as vulnerability scanners to identify weaknesses in the company's network infrastructure, including open ports, outdated software versions, or misconfigured settings. By scanning the network, the attacker can pinpoint potential entry points for exploitation.
2. Exploit identified vulnerabilities to gain initial access: Once vulnerabilities are identified, the attacker leverages exploit frameworks, which are collections of pre-written code or scripts designed to take advantage of specific vulnerabilities. By exploiting these weaknesses, the attacker gains initial access to the company's network, often through methods like remote code execution or privilege escalation.
3. Escalate privileges and move laterally through the network: With initial access secured, the attacker seeks to escalate their privileges within the network, granting

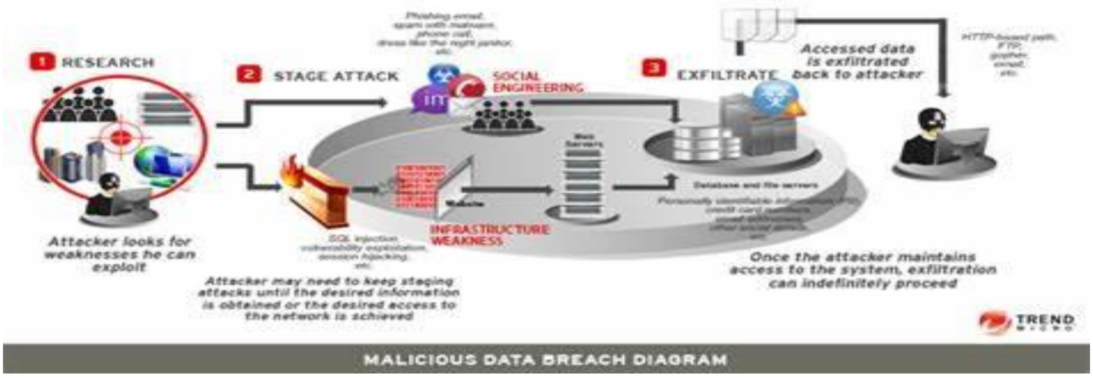
them greater control and access to sensitive resources. They may use various techniques and tools to move laterally through the network, such as exploiting trust relationships between systems or using stolen credentials to access additional machines.

4. Locate and exfiltrate sensitive data: Once inside the network, the attacker's final objective is to locate and exfiltrate sensitive data. They may use specialized tools for lateral movement to navigate through the network and identify valuable information repositories. Once identified, the attacker uses techniques such as data exfiltration tools or file transfer protocols to steal and transfer sensitive data outside the company's network.

3.3 Tools and Techniques:

- Vulnerability scanners: Vulnerability scanners are automated tools that scan networks for known vulnerabilities in software, configurations, or protocols. They provide a comprehensive assessment of potential weaknesses, allowing organizations to prioritize and remediate security issues before they can be exploited by attackers.
- Exploit frameworks: Exploit frameworks are collections of software tools, scripts, and exploits designed to automate the process of identifying and exploiting vulnerabilities in computer systems or networks. These frameworks often include exploits for known vulnerabilities in popular software applications, operating systems, or network devices, enabling attackers to quickly compromise targeted systems.
- Lateral movement tools: Lateral movement tools are used by attackers to navigate laterally across a network, moving from one compromised system to another to escalate privileges and access sensitive resources. These tools exploit vulnerabilities in network protocols, operating systems, or applications to pivot between systems and maintain persistence within the network.

4 Data Breaches:


1 RESEARCH
Attacker looks for weaknesses he can exploit
2 STAGE ATTACK
Phishing email, spam with malware, phone call, dress like the night janitor, etc.
SOCIAL ENGINEERING
SQL injection, vulnerability exploitation, session hijacking, etc.
Website
INFRASTRUCTURE WEAKNESS
Web Servers
Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved
3 EXFILTRATE
Accessed data is exfiltrated back to attacker
HTTP-based path, FTP, gopher, email, etc.
Database and file servers
Once the attacker maintains access to the system, exfiltration can indefinitely proceed
TREND MICRO
MALICIOUS DATA BREACH DIAGRAM

4.1 Objective:

Obtain access to confidential data stored by the company.

4.2 Steps:

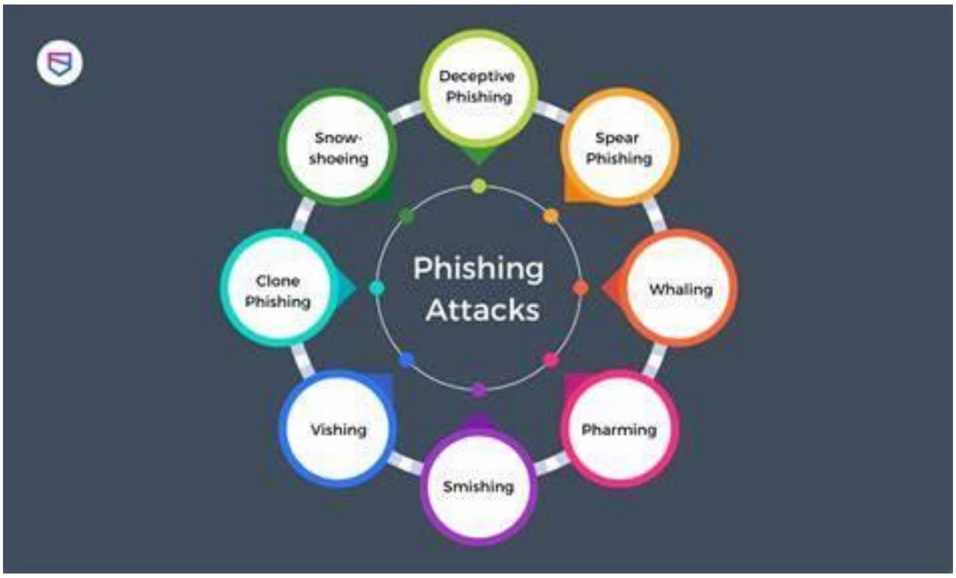
1. Identify weak points in the company's data storage systems: Attackers begin by assessing the company's data storage infrastructure to pinpoint vulnerabilities or weaknesses. They may use data scanning tools to analyze the organization's network and systems, looking for misconfigurations, unpatched software, or insecure access controls that could be exploited to gain unauthorized access to sensitive data.
2. Exploit vulnerabilities to gain unauthorized access: Once potential weak points are identified, attackers utilize exploit kits, which are packages of pre-written code designed to automate the exploitation of known vulnerabilities in software or systems. By exploiting these vulnerabilities, attackers can bypass security controls and gain unauthorized access to the company's data storage systems.
3. Locate and extract valuable data: With access to the company's data storage systems, attackers search for valuable data such as customer information, financial records, or intellectual property. They use various data exfiltration techniques to transfer the stolen data from the company's network to external servers or locations under their control, often employing encryption or obfuscation to avoid detection.

4.3 Tools and Techniques:

- Data scanning tools: Data scanning tools are software applications designed to scan and analyze an organization's network and systems for sensitive or confidential data. These tools can identify files or databases containing valuable information, such as credit card numbers, personal identifiers, or intellectual property, helping attackers prioritize their efforts and focus on high-value targets.

- Exploit kits: Exploit kits are collections of pre-packaged exploits, scripts, and tools that automate the process of exploiting known vulnerabilities in software or systems. Attackers deploy exploit kits to quickly and efficiently compromise target systems, bypassing security defenses and gaining unauthorized access to sensitive data. These kits often include exploits for commonly used software applications, web browsers, or operating systems.
- Data exfiltration techniques: Data exfiltration techniques are methods used by attackers to transfer stolen data from a compromised network to external servers or locations under their control. These techniques can include transferring data over encrypted channels, disguising data as legitimate traffic, or breaking up large files into smaller chunks to avoid detection. Attackers may also use covert channels or steganography to hide data within seemingly innocuous files or communications.

5 Phishing Attacks:



5.1 Objective:

Obtain login credentials or sensitive information through deceptive emails.

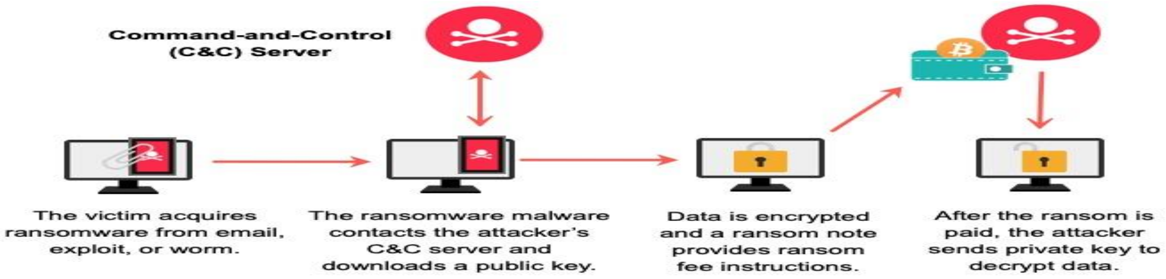
5.2 Steps:

1. Create convincing phishing emails tailored to target employees: Attackers craft phishing emails designed to appear legitimate and compelling, often using information gathered from social media or company websites to personalize the messages. These emails typically contain urgent requests, enticing offers, or alarming warnings to prompt recipients to take action, such as clicking on links or providing sensitive information.
2. Send phishing emails and monitor responses: Once the phishing emails are created, attackers use email spoofing tools to disguise the sender's identity and make the emails appear to come from trusted sources, such as colleagues or reputable organizations. They then send the phishing emails to targeted employees and monitor responses, tracking who interacts with the emails and how they respond.
3. Collect login credentials or other desired information: When recipients fall for the phishing emails and click on malicious links or enter their login credentials, attackers use credential harvesting techniques to collect the stolen information. This may involve redirecting victims to fake login pages that mimic legitimate websites, capturing entered credentials in real-time, or storing harvested data for later use.

5.3 Tools and Techniques:

- Phishing email generators: Phishing email generators are software tools that automate the creation of deceptive phishing emails. These tools often provide customizable templates and options for personalizing messages to increase their effectiveness. Attackers use phishing email generators to quickly create convincing emails tailored to specific target audiences, enhancing the success rate of their phishing campaigns.
- Email spoofing tools: Email spoofing tools allow attackers to manipulate email headers and sender information to make phishing emails appear to come from trusted sources or legitimate email addresses. By spoofing the sender's identity, attackers can deceive recipients into believing that the phishing emails are genuine, increasing the likelihood of successful social engineering attacks.
- Credential harvesting: Credential harvesting techniques involve capturing and collecting login credentials or sensitive information entered by victims in response to phishing emails or fake web forms. Attackers use various methods, such as phishing websites that mimic legitimate login pages, keylogging software that records keystrokes, or form grabbing techniques that intercept data submitted through web forms. harvested credentials can then be used for unauthorized access to accounts or for further exploitation in targeted attacks.

6 Ransomware Attacks:


Command-and-Control (C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware malware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends private key to decrypt data.

6.1 Objective:

Encrypt critical files and demand ransom for decryption.

6.2 Steps:

1. Gain initial access to the target network: Attackers first need to infiltrate the target network. They may accomplish this by exploiting vulnerabilities using tools like

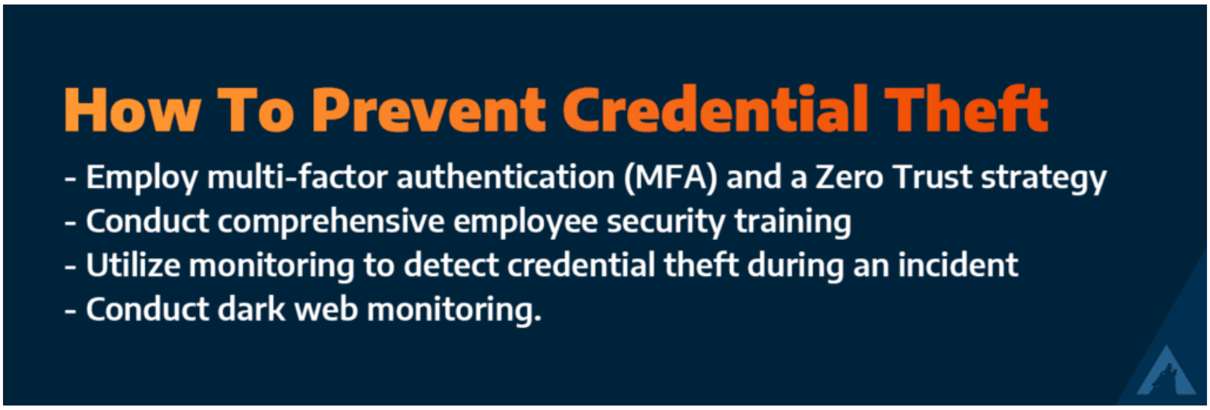
exploit kits, which automate the process of identifying and exploiting weaknesses in software or systems. Once inside, they can move laterally to find critical systems.

2. Deploy ransomware payload on critical systems: After gaining access, attackers deploy the ransomware payload onto critical systems within the network. This can be done using various methods, including exploiting unpatched software vulnerabilities or using social engineering tactics to trick users into downloading and executing malicious files.
3. Encrypt files and display ransom message: Once the ransomware payload is deployed, it begins encrypting files on the compromised systems, rendering them inaccessible to the victim. After encryption is complete, the ransomware typically displays a message demanding payment in exchange for the decryption key. This message often includes instructions on how to pay the ransom and regain access to the encrypted files.

6.3 Tools and Techniques:

- Ransomware-as-a-service platforms: Ransomware-as-a-service (RaaS) platforms are online services that allow individuals with limited technical expertise to create and distribute ransomware. These platforms provide a user-friendly interface and automated tools for generating customized ransomware payloads, enabling attackers to easily launch ransomware attacks without needing to develop their own malware from scratch.
- Exploit kits: Exploit kits are collections of pre-packaged exploits and tools designed to automate the process of identifying and exploiting vulnerabilities in software or systems. Attackers use exploit kits to quickly compromise target systems and gain initial access to the network, often exploiting vulnerabilities in web browsers, plugins, or other commonly used software.
- Payload delivery methods: Payload delivery methods refer to the techniques used by attackers to distribute and execute ransomware payloads on target systems. This can include methods such as phishing emails containing malicious attachments or links, drive-by downloads from compromised websites, or exploiting vulnerabilities in remote desktop protocols or file-sharing services. Once the ransomware payload is delivered and executed, it begins encrypting files on the victim's system.

7 Credential Theft:



How To Prevent Credential Theft

- Employ multi-factor authentication (MFA) and a Zero Trust strategy
- Conduct comprehensive employee security training
- Utilize monitoring to detect credential theft during an incident
- Conduct dark web monitoring.

7.1 Objective:

Obtain valid login credentials to gain unauthorized access.

7.2 Steps:

1. Identify targets with valuable credentials: Attackers first identify individuals within the target organization who have access to valuable systems or sensitive information. They may target employees with high-level privileges or individuals with access to critical infrastructure.

2. Use various methods to steal credentials (e.g., phishing, keylogging): Once targets are identified, attackers employ various techniques to steal their login credentials. Phishing involves sending deceptive emails or messages to trick individuals into revealing their credentials. Keyloggers are malicious software programs that record keystrokes, capturing usernames and passwords as they are entered.
3. Test stolen credentials to verify access: After obtaining credentials, attackers test them to verify their validity and assess the level of access they provide. They may use automated tools like password spraying, which involves attempting to authenticate with multiple accounts using commonly used passwords or known password lists.

7.3 Tools and Techniques:

- Keyloggers: Keyloggers are software programs or hardware devices that record keystrokes typed by a user on a compromised system. These tools capture login credentials, passwords, and other sensitive information as they are entered, allowing attackers to steal credentials without the victim's knowledge.
- Credential harvesting tools: Credential harvesting tools are software applications designed to automate the process of collecting login credentials from compromised systems or networks. These tools may use techniques such as capturing credentials from network traffic, extracting passwords from browser caches, or exploiting vulnerabilities in authentication mechanisms to harvest credentials en masse.
- Password spraying: Password spraying is a brute-force attack technique used to gain unauthorized access to accounts by attempting to authenticate with a large number of usernames and a small set of commonly used passwords or known password lists. This technique helps attackers evade detection by avoiding rapid or repeated login attempts with the same credentials, making it harder for security systems to detect and block suspicious activity

8 Conclusion

In summary, the red team playbook for data theft response offers a comprehensive framework for assessing and bolstering defenses against cyber threats. By simulating real-world attack scenarios like insider threats, external attacks, data breaches, phishing, ransomware, and credential theft, the playbook helps organizations identify vulnerabilities and improve their detection and response capabilities. Through a blend of reconnaissance, exploitation, and the use of various tools and techniques, teams can better prepare to detect, respond to, and mitigate data theft incidents. Regular updates and refinements to the playbook ensure adaptability to evolving threats, reinforcing the organization's ability to safeguard sensitive data and maintain business continuity. Ultimately, the red team playbook is an essential resource for strengthening security posture and mitigating the risks associated with data theft.

8 References

Insider Attack - https://www.revealrisk.com/wp-content/uploads/2023/02/Insider-Threat.png

External Attack- https://image2.slideserve.com/4325492/external-attack-l.jpg

Data Breach - https://th.bing.com/th/id/OIP.iGxtByysyOdxoYNKi3XATQAAAA?rs=1&pid=ImgDetMain

Phising Attack - https://th.bing.com/th/id/OIP.qD7APAjhv0EAuuEZlmKKdQAAAA?rs=1&pid=ImgDetMain

Ransomware Attack - https://assets.extrahop.com/images/blogart/ransomware/how-ransomware-works.jpg

Credential theft – https://arcticwolf.com/wp-content/uploads/2023/09/How-To-Prevent-Credential-Theft-1024x341.png

https://www.kiteworks.com/wp-content/uploads/2023/03/What-Are-Credential-Theft-Attacks.jpg