Document Reference:	UARTU-1	Effective Date:	6 May 2024
Document Name:	Unauthorised Access Red Team Usecases	Expiry Date:	6 May 2025

Unauthorised Access Red Team Usecases

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Liya Thomas
Next Review Date:	17 July 2024	Last Modified on:	2 May 2024

Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		2 May 2024	First Draft
0.2	Joel Daniel		6 May 2024	Cosmetic Changes
1.0	Liya Thomas	Joel Daniel	6 May 2024	Approved for Publishing

Table of Contents

1 Introduction

Unauthorized access incidents present grave threats to organizations, risking data breaches, financial harm, and reputational damage. Red team exercises play a pivotal role in emulating these attacks, evaluating security protocols, and fortifying incident response capabilities. This playbook serves as a comprehensive guide, delineating diverse unauthorized access scenarios. It furnishes clear objectives, systematic steps, essential tools, and effective techniques tailored to each attack type. By meticulously detailing these simulations, organizations can better understand their vulnerabilities, fortify defenses, and refine response strategies, ultimately fostering a robust security posture in the face of evolving threats.

2 Unauthorized Login Attempts

2.1 Objective:

Unauthorized login attempts aim to breach security defenses and gain illicit access to accounts, systems, or applications, leveraging techniques like password guessing, stolen credentials, or brute-force attacks. Such infiltration poses grave risks to data integrity and confidentiality, underscoring the importance of robust security measures.

2.2 Steps:

1 . Reconnaissance: In the reconnaissance phase, attackers meticulously gather intelligence about the target, including system configurations, user accounts, and potential vulnerabilities. This involves scanning network infrastructures, analyzing publicly available information, and conducting social engineering to ascertain valuable insights.

2. Password Guessing: Password guessing employs automated tools like Hydra, renowned for its effectiveness in launching systematic login attempts to crack passwords. Attackers utilize dictionaries, common passwords, and known patterns to guess credentials, exploiting weak password policies or user negligence.

3. Credential Stuffing: Credential stuffing automates the input of stolen credentials obtained from previous data breaches or leaks. Tools such as Sentry MBA streamline this process, enabling attackers to efficiently test large volumes of username-password pairs against various online services, exploiting users' tendencies to reuse passwords across multiple platforms.

4. Brute Force Attack: Brute force attacks, executed using tools like THC-Hydra, involve systematically trying every possible combination of usernames and passwords until the correct one is discovered. This method is resource-intensive but can be devastatingly effective against weak or improperly secured systems, emphasizing the importance of strong password policies and rate limiting.

5. Exploit Valid Credentials: Once valid credentials are obtained, attackers gain unauthorized access to the target system, potentially compromising sensitive data, installing malware, or further escalating their attack. Exploiting valid credentials underscores the significance of robust authentication mechanisms, continuous monitoring, and user education to mitigate the risk of insider threats or account compromise.

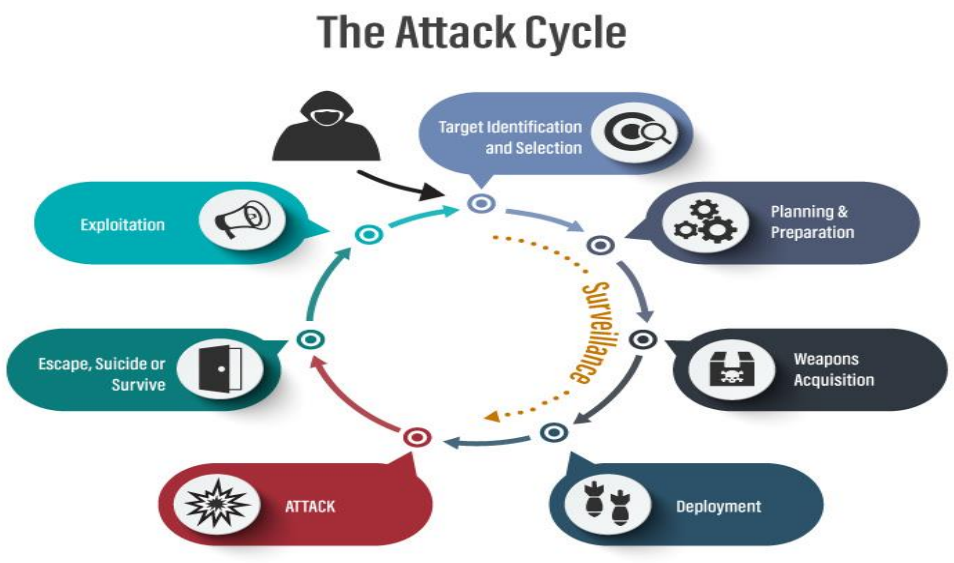
2.3 Tools and Techniques:

- Hydra: Hydra is a versatile and widely used tool in unauthorized login attempts. Its comprehensive features enable attackers to conduct efficient password guessing attacks across various protocols and services, aiding in the identification of weak authentication mechanisms.
- Sentry MBA: Sentry MBA is a specialized tool designed for credential stuffing attacks. Its automation capabilities streamline the process of testing stolen credentials

against multiple online services, maximizing the efficiency and scale of the attack while minimizing the manual effort required.

- THC-Hydra: THC-Hydra is renowned for its brute force capabilities, enabling attackers to systematically try millions of username-password combinations to gain unauthorized access. Its versatility and speed make it a formidable tool in penetrating even well-defended systems, highlighting the importance of implementing strong authentication measures and monitoring for suspicious activity.

3 Exploiting Vulnerabilities



©2022 TorchStone Global, LLC | www.torchstoneglobal.com

3.1 Objective:

The primary objective in exploiting vulnerabilities is to take advantage of weaknesses in hardware, software, or configurations to gain unauthorized access, posing significant risks to system integrity and confidentiality.

3.2 Steps:

1. Vulnerability Scanning:Vulnerability scanning, facilitated by tools like Nessus, involves thorough examination of target systems for known vulnerabilities, misconfigurations, or outdated software versions. This process yields insights into potential entry points for exploitation, forming the foundation of subsequent attack strategies.

2. Exploit Development:Upon identifying vulnerabilities during the scanning phase, attackers embark on exploit development. This entails crafting or acquiring exploit code tailored to specific vulnerabilities, creating payloads or scripts capable of leveraging weaknesses to gain unauthorized access to target systems.

3. Exploit Execution:Executing exploits using tools such as Metasploit automates the process of compromising vulnerable systems. Metasploit's extensive library of pre-built exploits streamlines the attack process, allowing attackers to launch attacks against a wide range of targets efficiently and effectively.

4. Persistence:Establishing persistence with tools like Meterpreter is crucial for maintaining access to compromised systems post-exploitation. Meterpreter enables attackers to maintain control over compromised infrastructure by offering a range of post-exploitation capabilities, including file system manipulation, privilege escalation, and network reconnaissance.

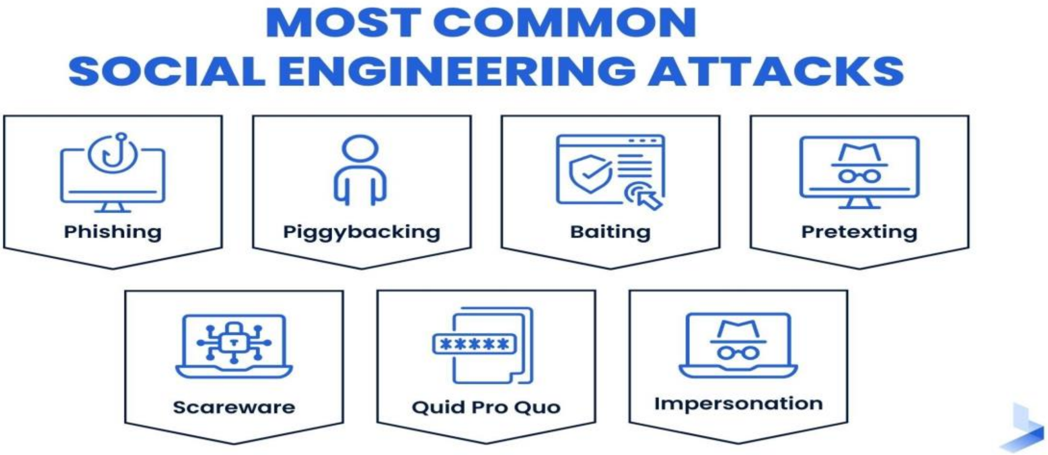
5. Cover Tracks:To evade detection and conceal the intrusion, attackers may delete logs or manipulate system records, effectively covering their tracks. This step is essential for hindering forensic investigation and attribution, prolonging the duration of unauthorized access.

3.3 Tools and Techniques:

- Nessus:Nessus is a powerful vulnerability assessment tool that identifies security vulnerabilities, configuration issues, and malware in systems. Its comprehensive scanning capabilities provide valuable insights into potential attack vectors, guiding the development of effective exploitation strategies.
- Metasploit:Metasploit is a widely-used framework for developing and executing exploits. Its extensive collection of tools and modules for penetration testing makes it a preferred choice for both red teams and attackers, streamlining the process of exploit execution and post-exploitation activities.

- Meterpreter: Meterpreter is a versatile post-exploitation tool used to establish persistence and gain deeper access to compromised systems. Its rich set of features enables attackers to maintain control over compromised infrastructure, facilitating further exploitation and data exfiltration.

4. Social Engineering Attacks



4.1 Objective:

Social engineering attacks aim to manipulate individuals into divulging private information or taking actions that compromise security, exploiting human psychology rather than technical vulnerabilities.

4.2 Steps:

1. Phishing: Phishing involves sending deceptive emails masquerading as legitimate sources to entice recipients into revealing sensitive information such as login credentials or financial details. These emails often contain links to malicious websites or attachments containing malware.

2. Pretexting: Pretexting involves fabricating scenarios or personas to deceive targets into disclosing information or performing specific actions. This technique relies on building

rapport and trust to manipulate individuals, often leading to the unwitting disclosure of sensitive information.

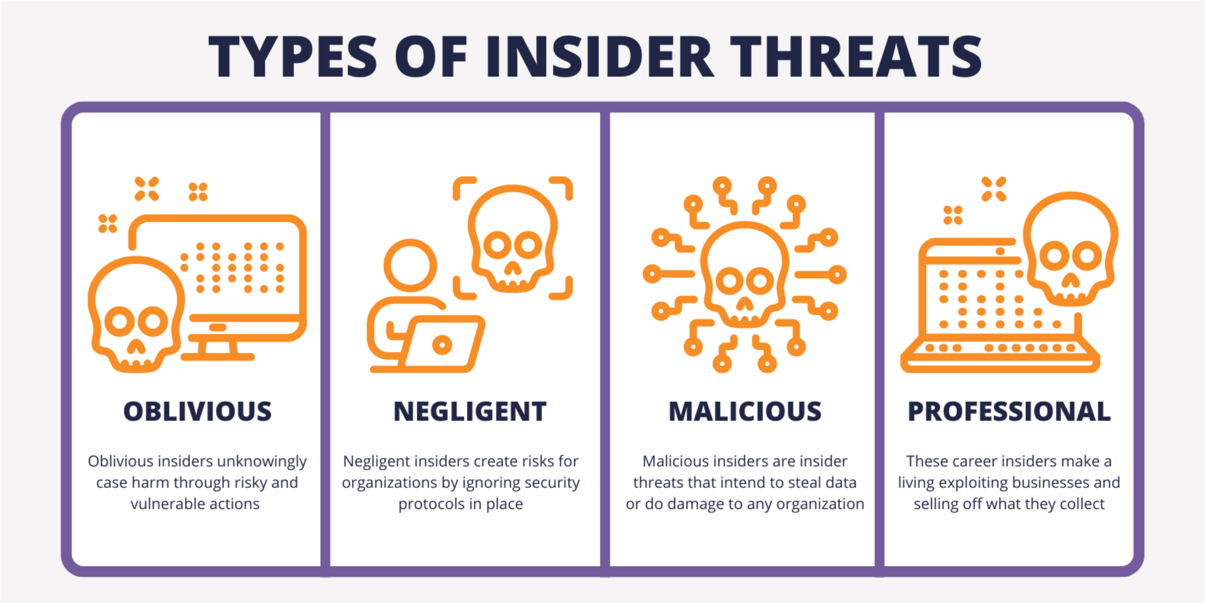
3. Baiting:Baiting involves enticing targets with promises of rewards or incentives to lure them into clicking on malicious links or downloading malware. This technique exploits human curiosity or greed, capitalizing on the willingness of individuals to engage with enticing offers.

4. Tailgating: Tailgating exploits physical security weaknesses by following authorized personnel into restricted areas without proper authentication. This technique relies on social engineering tactics to bypass access controls, allowing attackers to gain unauthorized access to secure facilities.

4.3 Tools and Techniques:

- Email Spoofing - Email spoofing involves forging the sender's email address to appear as if it originated from a trusted source, enhancing the credibility of phishing or pretexting attempts. This technique increases the likelihood of successful social engineering attacks by tricking recipients into believing that the email is legitimate.
- Social Engineering Toolkit (SET): The Social Engineering Toolkit (SET) is a comprehensive framework for automating social engineering attacks. It offers a range of tools and modules for phishing, credential harvesting, and exploiting human vulnerabilities, streamlining the process of launching and executing social engineering attacks.

5 Insider Threats



TYPES OF INSIDER THREATS

OBLIVIOUS

Oblivious insiders unknowingly case harm through risky and vulnerable actions

NEGLIGENT

Negligent insiders create risks for organizations by ignoring security protocols in place

MALICIOUS

Malicious insiders are insider threats that intend to steal data or do damage to any organization

PROFESSIONAL

These career insiders make a living exploiting businesses and selling off what they collect

5.1 Objective:

Insider threats involve exploiting authorized access to resources, data, or systems for malicious purposes, posing a significant risk to data confidentiality, integrity, and availability.

5.2 Steps:

1. User Activity Monitoring:Monitoring the activities of authorized users helps detect suspicious behavior or unauthorized access attempts, providing early warning signs of insider threats. This proactive approach enables organizations to identify and mitigate insider threats before they can cause significant harm.

2. Access Limits: Restricting access based on roles and responsibilities ensures that users only have access to the resources necessary to perform their job functions. By implementing access limits, organizations can minimize the risk of unauthorized data access or misuse by limiting the scope of user privileges.

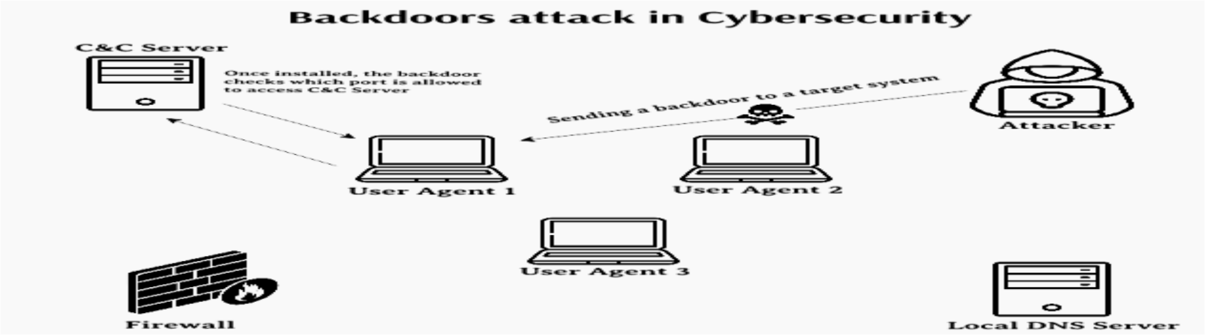
3. Least Privilege:Implementing the principle of least privilege ensures that users are granted only the minimum level of access required to perform their duties. By adhering to this principle, organizations can reduce the potential impact of insider threats by limiting the extent of access granted to users, thereby minimizing the risk of unauthorized data access or misuse.

4. Security Awareness Training: Training staff to recognize and report suspicious behavior or security incidents helps build a culture of security awareness within an organization. By educating employees about the potential risks posed by insider threats and empowering them to play an active role in defending against such threats, organizations can significantly enhance their security posture and mitigate the risk of insider attacks.

5.3 Tools and Techniques:

- User Activity Monitoring Tools: User activity monitoring tools track and log user actions, providing visibility into user behavior and identifying anomalies indicative of insider threats. By monitoring user activities, organizations can detect and investigate suspicious behavior, enabling them to mitigate the risk of insider threats proactively.
- Role-based Access Control (RBAC): RBAC restricts access to resources based on predefined roles and responsibilities, ensuring that users only have access to the information and systems necessary for their job functions. By implementing RBAC, organizations can enforce access controls effectively, minimizing the risk of unauthorized data access or misuse by limiting access to authorized users based on their roles and responsibilities.

6 Backdoor Access


Backdoors attack in Cybersecurity
C&C Server
Once installed, the backdoor checks which port is allowed to access C&C Server
Sending a backdoor to a target system
Attacker
User Agent 1
User Agent 2
User Agent 3
Firewall
Local DNS Server

6.1 Objective:

The primary objective of establishing backdoor access is to create covert entry points within systems or networks, enabling unauthorized access while evading detection.

6.2 Steps:

1. Secret Communication Channels: Establishing covert communication channels is crucial for maintaining stealthy access to compromised systems. By using encryption and obfuscation techniques, attackers can conceal communication traffic, making it difficult for security monitoring systems to detect unauthorized activity.

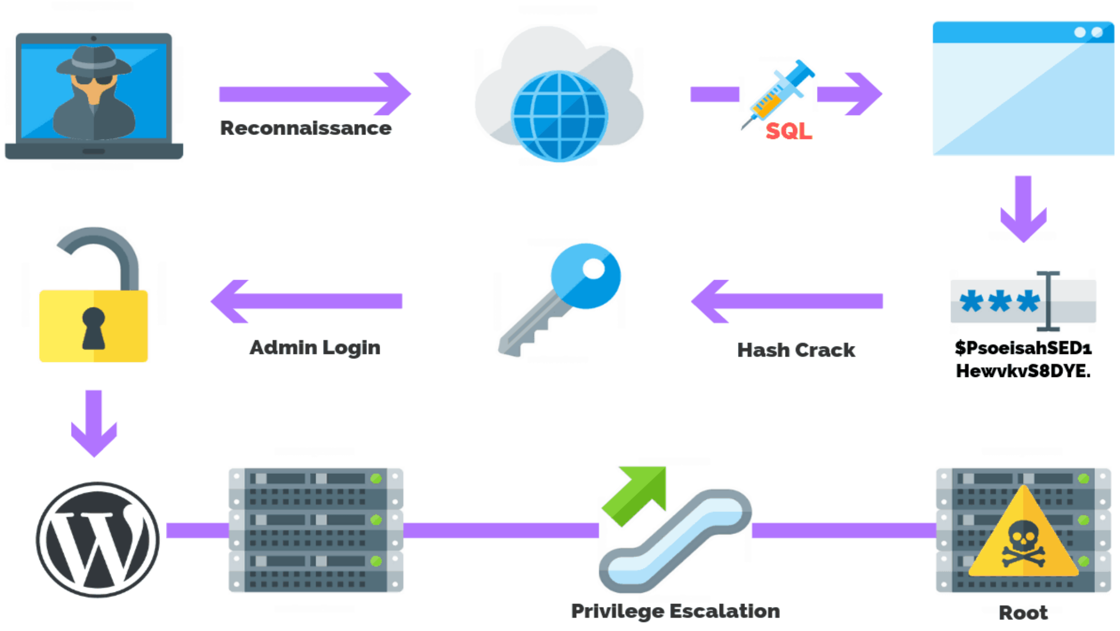
2. Default Credentials: Exploiting default credentials is a common tactic used by attackers to gain access to systems or devices. Manufacturers often use default usernames and passwords, which are widely known and easily exploitable if not changed by system administrators. Attackers capitalize on this oversight to gain unauthorized access without raising suspicion.

3. Exploiting Flaws: Taking advantage of vulnerabilities in systems or applications provides attackers with an opportunity to create backdoor access. By exploiting flaws such as buffer overflows, injection vulnerabilities, or insecure configurations, attackers can bypass security controls and establish persistent access to compromised systems.

6.3 Tools and Techniques:

- Covert Communication Tools: Tools designed for covert communication, such as steganography tools or custom-built communication protocols, enable attackers to conceal their activities within legitimate network traffic, making it challenging for security teams to detect unauthorized access.
- Exploit Development Frameworks:Exploit development frameworks provide attackers with the necessary tools and resources to develop exploits for targeting specific vulnerabilities. These frameworks streamline the process of identifying, developing, and deploying exploits, allowing attackers to exploit flaws effectively and establish backdoor access to target systems.

7 Privilege Escalation



7.1 Objective:

Privilege escalation involves increasing rights within a system or network, enabling attackers to access sensitive resources and perform unauthorized actions.

7.2 Steps:

1. Poor Authentication Procedures: Exploiting weak authentication procedures is a common tactic used by attackers to escalate privileges within a system. Weak passwords, insecure password storage mechanisms, and inadequate access controls can all be exploited to gain elevated privileges and access sensitive data or functionality.

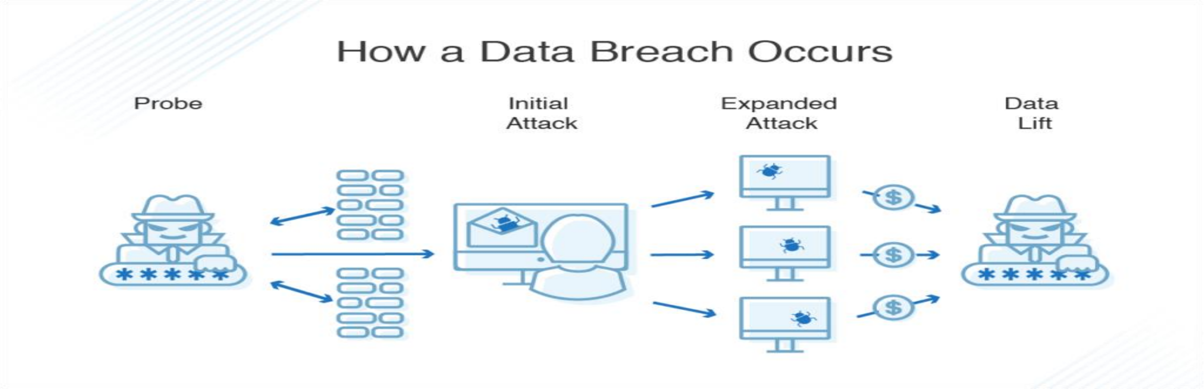
2. Misconfigured Permissions: Abusing misconfigured permissions is another method used by attackers to escalate privileges within a system. Improperly configured access control lists (ACLs), file system permissions, or user roles can provide attackers with unauthorized access to sensitive resources, allowing them to escalate privileges and perform malicious actions.

3. Software Vulnerabilities: Exploiting software vulnerabilities is a potent method for privilege escalation. Vulnerabilities such as buffer overflows, injection flaws, or insecure configuration settings can be exploited to execute arbitrary code with elevated privileges, enabling attackers to gain full control over a compromised system.

7.3 Tools and Techniques:

- Exploit Development Tools: Exploit development tools provide attackers with the necessary resources to identify and exploit software vulnerabilities effectively. These tools streamline the process of developing and deploying exploits, allowing attackers to escalate privileges within target systems and access sensitive resources.
- System Configuration Analysis Tools: System configuration analysis tools help attackers identify misconfigured permissions or inadequate access controls within target systems. By analyzing system configurations, attackers can identify potential privilege escalation opportunities and exploit them to gain elevated privileges.

8 Data Breaches



8.1 Objective:

The primary objective of data breaches is to obtain sensitive information without authorization, potentially leading to financial losses, reputational damage, and legal consequences.

8.2 Steps:

1. Social Engineering Attacks:Compromising credentials through social engineering attacks, such as phishing or pretexting, is a common tactic used by attackers to gain unauthorized access to sensitive information. By tricking users into divulging their credentials, attackers can bypass authentication controls and access sensitive data.

2. Exploiting Vulnerabilities: Gaining unauthorized access to databases or other data repositories by exploiting vulnerabilities is another method used by attackers to execute data breaches. Vulnerabilities such as SQL injection, cross-site scripting (XSS), or unpatched software flaws can be exploited to access and exfiltrate sensitive data without authorization.

3. Account Compromises: Exploiting weak authentication mechanisms or default credentials to compromise user accounts is a straightforward method for executing data breaches. By gaining unauthorized access to user accounts, attackers can access sensitive data stored within user profiles or personal information databases.

8.3 Tools and Techniques:

- Password Cracking Tools: Password cracking tools enable attackers to brute-force or guess user passwords, allowing them to gain unauthorized access to user accounts and execute data breaches. These tools leverage various techniques, such as dictionary attacks, brute-force attacks, or rainbow tables, to crack passwords and access sensitive information.
- SQL Injection Tools:SQL injection tools facilitate the exploitation of SQL injection vulnerabilities in web applications or database systems, enabling attackers to execute unauthorized SQL queries and access sensitive data stored within databases. These tools automate the process of identifying and exploiting SQL injection vulnerabilities, making it easier for attackers to execute data breaches.

Conclusion

Red team exercises are indispensable for identifying vulnerabilities, evaluating security controls, and enhancing incident response capabilities within organizations. By simulating unauthorized access scenarios, organizations can better prepare for real-world threats and mitigate risks effectively. Through systematic assessments and proactive defense strategies, organizations can strengthen their security posture and safeguard against evolving cyber threats

References

Unauthorized Login Attempts- https://4.bp.blogspot.com/_unRWYylMToA/TDRpKA0RxjI/AAAAAAAAAKo/gxuljxv0Sn0/s1600/login.jpg

Exploiting Vulnerabilities- https://www.torchstoneglobal.com/wp-content/uploads/2020/05/attack-cycle-diagram.jpg

Social Engineering Attacks - https://www.bitlyft.com/hs-fs/hubfs/Social%20Engineering%20Attacks.jpg?width=4800&height=2700&name=Social%20Engineering%20Attacks.jpg

insider threats - https://www.teramind.co/blog/wp-content/uploads/2022/06/What-Is-In-An-Insider-Threat-Blog-3.png

Backdoor Access - https://media.geeksforgeeks.org/wp-content/uploads/20220722123921/backdoor11.png

privilege escalation - https://purplesec.us/wp-content/uploads/2019/08/Privilege-Escalation-Attacks.png

Data breaches - https://www.dnsstuff.com/wp-content/uploads/2019/06/how-data-breach-occurs-1024x536.png