By: 9.2

SECURITY AUDITING

How to Conduct an Audit:

Conducting a security audit involves a systematic and comprehensive assessment of an organization's security controls, policies, and procedures.

- **Define Objectives and Scope:** Clearly define the objectives and scope of the security audit. Identify the systems, networks, applications, or processes that will be audited. Determine the specific areas of focus, such as access controls, network security, data protection, or compliance with regulations.

- **Gather Information:** Collect relevant documentation, policies, procedures, and technical specifications related to the audited systems or processes. This includes security policies, network diagrams, system configurations, access control lists, and incident response plans. Gain an understanding of the organization's security goals, regulatory requirements, and industry best practices.

- **Perform Risk Assessment:** Conduct a risk assessment to identify potential vulnerabilities and threats that could impact the audited systems. Assess the likelihood and potential impact of each risk and prioritize them based on their significance to the organization. This assessment helps determine the areas that require more attention during the audit.

- **Develop Audit Plan:** Create a detailed audit plan outlining the methodologies, tools, and techniques that will be used during the audit. Define the audit procedures, such as interviews, document reviews, vulnerability scanning, penetration testing, or configuration analysis. Establish a timeline and allocate resources accordingly.

- **Conduct Fieldwork:** Execute the audit plan by performing the agreed-upon procedures. This may involve interviewing key personnel, reviewing security controls, assessing technical configurations, examining logs and records, and conducting vulnerability assessments or penetration tests. Collect evidence and document observations.

- **Analyse Findings:** Analyse the collected data and evidence to identify security weaknesses, vulnerabilities, or non-compliance with policies and standards. Evaluate the effectiveness of existing security controls and processes. Compare the findings against established benchmarks, industry best practices, and regulatory requirements.

- **Prepare Audit Report:** Prepare a comprehensive audit report summarizing the findings, observations, and recommendations resulting from the audit. Clearly document the identified vulnerabilities, risks, and non-compliance issues. Provide actionable recommendations for improving security controls, policies, or procedures. Prioritize recommendations based on their potential impact and urgency.
- **Communicate Results:** Present the audit report to the relevant stakeholders, including management, IT teams, and other key personnel. Clearly communicate the findings, risks, and recommendations in a concise and understandable manner. Address any questions or concerns and seek feedback or input from stakeholders.

- **Monitor and Follow Up:** Track the implementation of recommended actions and improvements based on the audit findings. Monitor progress and ensure that identified vulnerabilities are remediated and control gaps are addressed. Conduct periodic reviews to assess the effectiveness of implemented measures and monitor changes in the organization's security posture.

- **Continual Improvement:** Use the audit findings as lessons learned to enhance the organization's overall security posture. Continually update and improve security policies, controls, and procedures based on emerging threats, industry trends, and regulatory changes. Regularly schedule security audits to maintain a proactive approach to security.

Red Team Audit:

A Red Team audit is meant to simulate a real attack in order to test the global security level of the information system and the awareness of the employees. The objective is to demonstrate the potential consequences of an attack, and to test the reactivity of the defense teams. It differs from a penetration test because it doesn't limit itself to listing vulnerabilities on a delimited perimeter.

- It targets an entire ecosystem: information system and employees.
- It is less limited in its execution perimeter, just like a real-life attack.

The Red Team audit can be seen as a combination of attack scenarios and objectives to accomplish.
A few examples are:

- Remote intrusion: identifying and exploiting every available public resource, such as websites, message interfaces...
- User Phishing: phishing mails, dropping malicious USB drives near the employee's paths...
- Non-destructive physical intrusion in the customer's office to connect a device to the client's network.

Only a few of the customer's employees are informed of this audit, and it's generally done over a relatively long period, typically a few months, so the customer cannot predict when the different scenarios will be accomplished, and therefore challenge the security in real-life conditions.

Some of the methods that can be done:

Recon:

The recon phase is a lot bigger than in a regular audit. The reason being that we don't just map out the computer resources and information system, but also identify the workers we could compromise later during the audit. For this, we conduct multiple operations with the goal of:

- identify the company workers based on an organization chart on the company website
- identify the company workers based on information's posted on social networks
- identify the company workers with large permissions and access to the information system, such as administrators, or IT support
- identify the company workers with lesser computer/security skills such as secretaries or enterprise responsible
- identify computer technologies used based on job offers posted on the internet
- and of course, identifying publicly exposed services: webmail, VPN access, extranet, firewall or server administration...

External Resource attack:

This stage amounts to an external audit and a web application audit.

Social Engineering:

This is one of the main differences between a regular audit and a Red Team audit: we don't solely try to exploit software vulnerabilities, but also make use of the lack of awareness of the employees. Thanks to the information's gathered during the recon stage, we'll try to penetrate your information system using the employees.

A few examples of the methods used:

- Sending phishing emails crafted to target one or more employees
- Calling employees claiming to be a technical support agent
- Dropping malicious USB drives close to the office
- Dropping flyers at the reception offering advantages for local shops or restaurants

Penetrating the office:

This stage can have multiple objectives. On one hand, we can test the welcome process for outsiders and see whether it's possible to access restricted areas by using the employees' lack of awareness. On the other hand, we'll try to set up a device on the internal network to get a remote access to the network, and initiate the next stage without needing to physically stay in the office.

There are multiples means to this end:

- intrusion using concealed doors such as service doors, garages...
- intrusion using improperly closed windows
- intrusion by mingling with a group of legitimate employees
- intrusion through the main entrance using pretences such as a delivery, an urgent need...

Internal resources attack:

If we managed to connect a device on your network to get remote access, this stage amounts to a internal network security audit (LAN).

Some common security auditing activities performed by a red team:

- **Wireless Network Testing:** Red teams evaluate the security of wireless networks by attempting to gain unauthorized access to wireless access points, routers, or other wireless infrastructure. They also assess the effectiveness of encryption protocols and authentication mechanisms.

- **Application Security Assessment:** Red teams assess the security of web applications, mobile applications, or other software solutions. They identify vulnerabilities like code injection, insecure authentication, or inadequate access controls that could be exploited by attackers.

- **Physical Security Assessment:** Red teams evaluate the physical security measures in place, such as access controls, CCTV systems, alarm systems, and employee identification systems. They attempt to breach physical security barriers, gain unauthorized entry to restricted areas, or tamper with critical equipment.

- **Threat Modelling:** Red teams analyse an organization's systems, processes, and assets to identify potential threats and prioritize risks. They simulate targeted attacks based on real-world threat scenarios and assess the organization's ability to detect and respond to them effectively.

- **Security Policy Review:** Red teams review an organization's security policies, procedures, and guidelines to identify gaps or inconsistencies. They assess if the policies align with industry best practices and regulatory requirements and provide recommendations for improvements.

- I**ncident Response Assessment:** Red teams simulate security incidents to assess the effectiveness of an organization's incident response capabilities. They evaluate the detection, containment, eradication, and recovery processes, and provide feedback to enhance the organization's incident response capabilities.

LOG FILING

Log filing is the process of collecting and storing all the data that is generated by an organization's IT systems. This data can include things like network traffic, system logs, and application logs. Log files can be used to track user activity, identify security incidents, and troubleshoot problems.

How to conduct log management:

During a red team exercise, log filing plays a crucial role in capturing and documenting activities, findings, and evidence. It helps in maintaining a detailed record of actions taken during the exercise, which can be analysed and reviewed later. Here's a general process for conducting log filing in a red team exercise:

- **Define Objectives:** Clearly define the objectives of the red team exercise, including the scope, target systems, and specific goals. This will help determine the types of logs to be collected.

- **Identify Relevant Logs:** Determine which logs are relevant to the exercise based on the target systems, network infrastructure, and available resources. Common log sources include operating systems, network devices, applications, and security tools.
- **Configure Log Collection:** Configure the target systems and logging infrastructure to ensure logs are generated and captured appropriately. This may involve enabling auditing, logging, and monitoring features on the target systems or deploying network-based logging solutions.

- **Determine Log Retention:** Decide on the duration for which logs will be retained. Consider regulatory requirements, organizational policies, and the duration needed for analysis and review after the exercise. Longer retention periods allow for more comprehensive analysis.

- **Capture Logs:** During the red team exercise, ensure that the configured logging mechanisms are actively capturing the relevant logs. Monitor the log collection process to identify any issues or gaps in the captured logs. Regularly check the logging infrastructure to verify that logs are being generated and stored correctly.

- **Document Activities:** Maintain a separate log file to document the activities performed during the exercise. This log file should include details such as the date and time of each activity, the specific actions taken, the tools or techniques used, and any outcomes or findings. Be thorough and accurate in recording the information.

- **Organize and Analyse Logs:** Once the red team exercise is complete, gather and consolidate all captured logs from different sources. Organize the logs in a central location or a dedicated log management system. Use appropriate log analysis tools and techniques to review and analyse the collected logs for any indicators of compromise or suspicious activities.

- **Reporting and Lessons Learned:** After analysing the logs, prepare a comprehensive report detailing the red team exercise findings, including any vulnerabilities, exploits, or weaknesses identified. Document the lessons learned,

recommendations for improvement, and suggested mitigation measures based on the exercise outcomes.

Red Team Log Filing:

During a red team exercise, the following log filing activities are typically performed by the red team:

1. **Initial Assessment:** The red team conducts an initial assessment of the target systems and network infrastructure to identify potential log sources and determine the logging capabilities already in place.

2. **Logging Configuration:** The red team configures the target systems, network devices, and applications to generate and capture relevant logs. This may involve enabling auditing, logging, and monitoring features, adjusting log levels, and configuring log formats.

3. **Activity Documentation:** The red team maintains a log file to document their activities throughout the exercise. This log file includes details such as the date and time of each activity, the specific actions taken, the tools or techniques used, and any outcomes or findings.

4. **Log Collection:** The red team ensures that the configured logging mechanisms are actively capturing the relevant logs during the exercise. They monitor the log collection process to identify any issues or gaps in the captured logs and make adjustments as needed.

5. **Log Analysis:** Once the red team exercise is complete, the red team gathers and consolidates all captured logs from different sources. They organize the logs in a central location or a dedicated log management system for further analysis.

6. **Log Review:** The red team reviews the captured logs to identify any indicators of compromise or suspicious activities. They analyse the logs to understand the sequence of events, identify potential vulnerabilities, and gather evidence of successful or attempted attacks.

7. **Reporting:** The red team prepares a comprehensive report detailing their findings based on the analysis of the logs. This report includes information about identified vulnerabilities, exploited weaknesses, successful compromises, and recommendations for improvement.

8. **Post-Exercise Cleanup:** After the red team exercise, the red team ensures that all logs generated during the exercise are properly archived and securely stored. They remove any traces of their activities from the target systems and network infrastructure.

SCENARIO-BASED ADVERSARIAL SIMULATION

Scenario-based adversarial simulation refers to a method used by red teams to simulate realistic attack scenarios to assess an organization's security defences, detection capabilities, and incident response procedures. It involves creating a controlled environment where the red team, acting as adversarial entities, attempts to breach the organization's systems and networks using techniques that real attackers might employ.

The purpose of scenario-based adversarial simulation is to identify vulnerabilities, weaknesses, and gaps in an organization's security posture. By simulating real-world attack scenarios, the red team can provide valuable insights into the effectiveness of the organization's security controls and help identify areas that require improvement.

HOW DOES RED-TEAM CONDUCT SCENARIO-BASED ADVERSARIAL SIMULATION?

1. **Planning: The red team starts by collaborating with the organization's stakeholders to understand their goals, objectives, and critical assets. They identify potential attack scenarios that align with the organization's threat landscape, such as advanced persistent threats (APTs), ransomware attacks, or data breaches.**

2. **Reconnaissance: The red team conducts extensive reconnaissance to gather information about the organization's external and internal infrastructure. They may perform open-source intelligence (OSINT) gathering, scanning for publicly available information, identifying potential attack vectors, and mapping the organization's network and systems.**

3. **Vulnerability Analysis: Using the information gathered during reconnaissance, the red team performs vulnerability analysis to identify weaknesses in the organization's systems, applications, or infrastructure. They employ tools like vulnerability scanners, network sniffers, or manual analysis techniques to discover potential vulnerabilities and misconfigurations.**

4. **Exploitation: Once vulnerabilities are identified, the red team attempts to exploit them to gain unauthorized access to the organization's systems or networks. They may employ techniques like exploiting software vulnerabilities, leveraging social engineering tactics, or using phishing emails to trick employees into running malicious code.**

5. **Persistence and Lateral Movement: Once inside the organization's network, the red team aims to establish persistence by maintaining access and moving laterally across the network. They may use techniques like privilege escalation, password cracking, or compromising weakly protected systems to gain control over critical infrastructure components.**

6. **Data Exfiltration: The red team attempts to exfiltrate sensitive data from the organization without being detected. They might utilize techniques like data encryption, steganography (hiding data within other files), or covert communication channels to transfer data out of the organization's network.**

7. **Post-Attack Cleanup: After completing the simulated attack, the red team removes all traces of their presence from the organization's systems and network. They may delete logs, restore compromised files, and cover their tracks to make it difficult for the organization's incident response teams to identify the attack.**

8. **Reporting: Finally, the red team documents their findings, including the vulnerabilities exploited, techniques used, and recommendations for improving the organization's security posture. They provide a detailed report to the organization's stakeholders, highlighting areas for improvement and suggesting mitigation strategies.**

HOW DOES THIS VARY FROM SECURITY AUDIT?

scenario-based adversarial simulation focuses on simulating real-world attacks to assess an organization's detection and response capabilities, while security audits take a broader and more comprehensive approach to evaluate an organization's overall security posture, adherence to standards, and compliance with regulations. Both activities serve different purposes and provide unique insights into an organization's security landscape.

WHY DO WE NEED SBAS?

1. **Real-world Threat Simulation: By simulating real-world attack scenarios, red teams can provide organizations with a realistic understanding of their security posture. This approach helps identify vulnerabilities and weaknesses that may not be easily apparent through traditional security assessments.**

2. **Training and Awareness: Engaging in scenario-based adversarial simulation provides organizations with a valuable learning experience. It helps raise awareness among employees about potential threats and attack techniques, and allows them to gain practical knowledge about incident response procedures and mitigation strategies.**

3. **Continuous Improvement: Scenario-based adversarial simulation promotes a culture of continuous improvement within an organization. By regularly conducting these assessments, organizations can iteratively enhance their security defences, refine incident response procedures, and stay updated with the evolving threat landscape.**

SECURITY AWARENESS TRAINING

Security awareness training is an essential component of an organization's security strategy. It aims to educate employees and stakeholders about potential security risks, best practices, and their roles and responsibilities in maintaining a secure environment. Red teams often contribute to security awareness training by providing valuable insights and conducting interactive sessions.

HOW DOES RED TEAM CONDUCT SECURITY AWARENESS TRAINING:

1. Identifying Risks: Red teams assist in identifying the specific security risks and threats that an organization faces. They can share real-world examples and demonstrate common attack vectors, helping employees understand the potential impact of security breaches.

2. Creating Engaging Content: Red teams collaborate with training specialists to develop engaging and interactive training materials. These may include presentations, videos, quizzes, and simulations that convey security concepts in an easily understandable manner. By leveraging their expertise, red teams ensure that the content remains relevant and up-to-date.

3. Addressing Common Threats: Red teams focus on highlighting and explaining the most prevalent security threats faced by organizations. This includes topics such as phishing attacks, social engineering, password hygiene, physical security, data protection, and safe browsing habits. They provide practical tips and techniques for recognizing and mitigating these threats.

4. Simulating Attacks: Red teams conduct simulated attacks as part of security awareness training. These exercises can involve sending mock phishing emails, making simulated social engineering calls, or performing physical security tests. Such activities help employees experience realistic scenarios and learn to recognize and respond appropriately to potential threats.

5. Tailoring Training: Red teams work with the organization's training team to customize the content and delivery of security awareness training. They consider the specific industry, regulatory requirements, and unique security challenges faced by the organization. This tailored approach ensures that training materials are relevant and resonate with employees.

6. Measuring Effectiveness: Red teams can assist in evaluating the effectiveness of security awareness training programs. They can conduct post-training assessments to measure knowledge retention, identify areas for improvement, and provide recommendations to enhance the training program's impact.

WHY DO WE NEED SECURITY AWARENESS TRAINING:

1.Human Weaknesses: Employees are often considered the weakest link in an organization's security posture. Security awareness training helps address this vulnerability by educating employees about potential risks and teaching them how to recognize and respond to security threats effectively. It empowers individuals to make informed security decisions and take appropriate actions to protect sensitive data and systems.

2.Data Protection: Employees handle sensitive data daily, and their actions can significantly impact data protection. Security awareness training educates employees about the importance of safeguarding data, using secure practices for data handling and storage, and complying with data protection policies. This reduces the risk of data breaches, unauthorized access, and data loss.

3.Mitigating Insider Threats: Insider threats, whether intentional or unintentional, can pose significant risks to an organization's security. Security awareness training raises awareness about the signs of potential insider threats, such as unauthorized access attempts, unusual behaviour, or data exfiltration. It also promotes a culture of vigilance and encourages employees to report any suspicious activities promptly.