# PURPLE PLAYBOOK

For RightPoint

Malicious Network Scanning ........ 3

Introduction: ........ 3

Roles and Responsibilities: ........ 3

Scope and Rules of Engagement: ........ 4

Planning and Preparation: ........ 5

Metrics and Reporting: ........ 6

Man in the Middle ........ 8

Introduction: ........ 8

Roles and Responsibilities: ........ 8

Exercise Scope and Rules of Engagement: ........ 9

Planning and Preparation: ........ 10

Metrics and Reporting: ........ 11

Password Cracking Attempts ........ 13

Roles and Responsibilities: ........ 13

Exercise Scope and Rules of Engagement: ........ 14

Planning and Preparation: ........ 15

Metrics and Reporting: ........ 17

DoS Attacks ........ 18

Introduction: ........ 18

Roles and Responsibilities: ........ 18

Exercise Scope and Rules of Engagement: ........ 19

Planning and Preparation: ........ 21

Metrics and Reporting: ........ 22

SQL Injections ........ 24

Introduction: ........ 24

Roles and Responsibilities: ........ 24

Exercise Scope and Rules of Engagement: ........ 25

Planning and Preparation: ........ 25

Metrics and Reporting: ........ 26

Phishing ........ 28

Introduction: ........ 28

Roles and Responsibilities: ........ 28

Scope and Rules of Engagement: ........ 29

Planning and Preparation: ........ 30

Metrics and Reporting: ........ 31

# *Malicious Network Scanning*

## Introduction:

The RightPoint purple team playbook is a comprehensive guide designed to enhance cybersecurity resilience within the organization. Combining the offensive capabilities of the red team with the defensive expertise of the blue team, the purple team conducts collaborative exercises to identify vulnerabilities, test defences, and improve overall security posture. This playbook addresses the threat of malicious network scanning, provides strategies to protect against it, emphasizes the importance of employee training, and ensures safety for the wider organization during training exercises.

## Roles and Responsibilities:

**Purple Team:**
The purple team leader serves as the overall coordinator and facilitator of the purple team exercises. They are responsible for managing the collaborative efforts between the red and blue teams, ensuring effective communication, and overseeing the execution of the exercises. The Purple team leader should possess a deep understanding of RightPoint's security landscape, risks, and business objectives. They are accountable for driving improvements in the organization's security posture based on the findings from the exercises.

**Red Team:**
The red team is responsible for conducting offensive operations to simulate real-world attacks on RightPoint's network. Their objective is to identify vulnerabilities, weaknesses, and potential entry points that threat actors may exploit. The red team should employ sophisticated attack techniques and tactics, leveraging their expertise to emulate various threat scenarios. They collaborate with the blue team by sharing insights, recommendations, and potential remediation strategies to enhance the organization's defences.

**Blue Team:**
The blue team is responsible for detecting, responding to, and defending against simulated attacks conducted by the red team. They actively monitor and analyse the network for signs of compromise, promptly respond to incidents, and implement defence strategies. The Blue team collaborates with the red team to identify gaps in the organization's defences and develop remediation plans. Their focus is on improving incident response capabilities, implementing robust security measures, and ensuring the ongoing security of RightPoint's network.

**IT and Security Personnel:**
IT and security personnel play a vital role in supporting the purple team exercises. They assist in implementing technical controls, monitoring the network for potential threats, and responding to incidents as part of the blue team. They also collaborate closely with the purple team leader, red team, and executive sponsor to ensure the exercises align with the organization's security objectives. IT and security personnel contribute their expertise to the continuous improvement of security policies, procedures, and technologies.

**Executive Sponsor:**
The executive sponsor provides high-level support and advocacy for the purple team exercises. They champion the importance of the exercises to the organization's overall security strategy and allocate necessary resources for their successful execution. The executive sponsor guides and aligns the purple team's activities with the broader business objectives, fostering a culture of security awareness and continuous improvement throughout the organization.

## Scope and Rules of Engagement:

**Exercise Scope:**
The scope of the purple team exercises will encompass a comprehensive evaluation of RightPoint's network infrastructure, systems, applications, and associated security controls. This includes both internal and external components, such as on-premises systems, cloud environments, remote access mechanisms, and any other relevant network assets. The exercises will focus on simulating realistic attack scenarios to identify vulnerabilities, validate the effectiveness of defensive measures, and enhance the organization's security posture.

**Rules of Engagement:**

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. Authorized Targets:**
The purple team exercises will be limited to authorized targets within RightPoint's network infrastructure. Participants must strictly adhere to the predefined scope and avoid any attempt to access or compromise unauthorized systems, data, or infrastructure.

**3. Legal and Compliance Considerations:**
The purple team exercises will be conducted in full compliance with applicable laws, regulations, and organizational policies. Any actions that could potentially violate legal or ethical boundaries, disrupt normal business operations, or cause harm to systems or data are strictly prohibited.

**4. Communication and Coordination:**
Effective communication and coordination among the purple team leader, red team, blue team, IT and security personnel, and executive sponsor are essential. Regular meetings, progress updates, and collaboration sessions should be scheduled to exchange information, address challenges, and ensure alignment with organizational goals.

**5. Incident Response and Reporting**:
In the event of a security incident or unexpected impact during the exercises, participants should follow established incident response procedures. Prompt reporting, thorough documentation, and analysis of any findings or incidents are critical for post-exercise analysis and improvement of security measures.

**6. Limitations and Constraints:**
The purple team exercises may have limitations and constraints defined in advance to

prevent unintended disruptions or negative impacts on critical business processes, production systems, or third-party networks. Participants must operate within these limitations and consider the potential consequences of their actions.

**7. Continuous Improvement:**
The purple team exercises aim to drive continuous improvement in the organization's security posture. Lessons learned, best practices, and identified vulnerabilities should be documented, shared, and used to enhance security policies, procedures, and technologies.

## Planning and Preparation:

Effective planning and preparation are crucial for the successful execution of purple team exercises, particularly in managing the roles of the blue and red teams in addressing malicious network scanning. This section provides guidance on the key steps involved in planning and preparing for these exercises.

**1. Define Objectives:**
Clearly articulate the objectives of the purple team exercises related to addressing malicious network scanning. These objectives may include identifying vulnerabilities in network defences, testing incident response capabilities, and improving the organization's ability to detect and mitigate network scanning activities.

**2. Scoping and Target Selection:**
Determine the scope of the exercises by identifying specific systems, networks, and assets that will be targeted for simulated malicious network scanning. Consider both internal and external components of the network infrastructure to ensure comprehensive coverage. It is crucial to obtain proper authorization and align the scope with legal and compliance requirements.

**3. Resource Allocation:**
Allocate necessary resources, including personnel, tools, and equipment, to support the blue and red teams during the exercises. Ensure that team members have the required expertise and access to appropriate tools for their respective roles.

**4. Rules of Engagement:**
Establish clear rules of engagement for the blue and red teams, outlining the permissible actions, targets, and constraints. Specify what techniques and tools are allowed or prohibited during the exercises. Define communication channels, incident reporting procedures, and guidelines for handling any unintended impact on live systems.

**5. Information Sharing:**
Foster open and transparent communication between the blue and red teams to promote knowledge exchange and collaboration. Encourage the sharing of insights, findings, and recommendations throughout the exercises to facilitate joint problem-solving and improvement of defences against malicious network scanning.

**6. Test Scenarios:**
Develop realistic test scenarios that simulate different types of malicious network scanning activities. Consider various attack vectors, such as port scanning, vulnerability scanning, and

reconnaissance techniques. Design scenarios that align with the organization's specific threat landscape and industry best practices.

**7. Timelines and Milestones:**
Establish clear timelines and milestones for the purple team exercises. Define key deliverables, deadlines, and review points to ensure progress tracking and accountability. Regularly evaluate the status of the exercises and adjust plans if necessary to stay on track.

**8. Documentation and Reporting:**
Establish a documentation framework to capture the findings, actions taken, and lessons learned during the exercises. Document vulnerabilities, remediation strategies, and recommendations for improvement. Generate comprehensive reports to communicate exercise outcomes, highlighting areas of success and opportunities for further enhancement.

**9. Post-Exercise Analysis:**
Conduct a thorough analysis of the exercise results, including identified vulnerabilities, response effectiveness, and overall performance. Evaluate the success of the blue team's defence mechanisms against malicious network scanning and assess the red team's ability to exploit vulnerabilities. Use this analysis to drive continuous improvement in the organization's security posture.

## Metrics and Reporting:

**1. Vulnerability Discovery:**
Measure the number and severity of vulnerabilities discovered during the malicious network scanning exercise. Track metrics such as the total number of vulnerabilities identified, their criticality levels, and the time taken to detect and remediate them. This provides insights into the organization's overall vulnerability landscape and the efficiency of vulnerability management processes.

**2. Response Time:**
Evaluate the response time of the blue team in identifying and responding to the simulated malicious network scanning activity. Measure the time taken to detect and report the scanning attempts, as well as the speed of incident response and mitigation actions. These metrics reflect the organization's ability to swiftly identify and address potential threats.

**3. Incident Handling:** Assess the effectiveness of the blue team's incident handling and response capabilities. Measure metrics such as the number of incidents generated during the exercise, the average time to investigate and resolve them, and the accuracy of incident categorization and prioritization. These metrics provide insights into incident management processes and help identify areas for improvement.

**4. Security Controls:** Evaluate the effectiveness of existing security controls in detecting and preventing malicious network scanning activities. Measure the performance of intrusion detection and prevention systems (IDS/IPS), firewall rules, and network monitoring tools. Assess metrics such as the number of successful scans evading detection, false positive rates, and the overall capability to thwart scanning attempts.

**5. Network Visibility:** Determine the level of network visibility achieved during the exercise. Measure metrics such as the percentage of network traffic monitored, the coverage of network monitoring tools, and the ability to detect anomalous behaviours indicative of scanning activities. These metrics reflect the organization's ability to monitor and identify suspicious network traffic.

**6. Remediation Metrics:**
Track the effectiveness and efficiency of remediation efforts following the identification of vulnerabilities. Measure metrics such as the average time to patch or mitigate vulnerabilities, the closure rate of identified issues, and the adherence to vulnerability management processes. These metrics help assess the organization's ability to prioritize and address vulnerabilities promptly.

**7. Reporting Requirements:**
Define reporting requirements for the malicious network scanning exercise. Reports should include an executive summary, methodology, key findings, and recommendations for remediation. Present metrics in a clear and concise manner, accompanied by visualizations to enhance comprehension. Include insights on vulnerabilities discovered, response times, and the overall security posture.

**8. Continuous Improvement:**
Leverage the metrics and insights gathered from the exercise to drive continuous improvement. Identify recurring vulnerabilities, bottlenecks in incident response, or gaps in security controls. Use the findings to enhance security policies, update detection mechanisms, and prioritize security investments.

# *Man in the Middle*

## Introduction:

In this exercise, teams will verify RightPoint's ability to protect against Man-in-the-Middle (MITM) attacks through via their implementation of robust encryption protocols. Additionally, we will highlight the significance of regular training exercises, conducted in a safe environment, to ensure your team's readiness in detecting and responding to MITM attacks. By following the strategies outlined in this playbook, you can strengthen your defence mechanisms and mitigate the risks associated with MITM attacks, safeguarding your valuable assets.

## Roles and Responsibilities:

**Purple Team:**
The purple team oversees the entire exercise, ensuring it aligns with organizational objectives. They facilitate communication between the Red Team and Blue Team, evaluate security controls and incident response procedures, and provide regular updates and reports to the executive sponsor.

**Red Team:**
The red team develops and executes realistic MITM attack scenarios, simulating various attack vectors and techniques. They continuously update their tactics to emulate sophisticated threat actors, document vulnerabilities exposed during the exercise, and provide detailed findings on attack paths and potential impact.

**Blue Team:**
The blue team monitors network traffic and system logs to detect and identify MITM attacks. They implement and maintain robust security controls, such as intrusion detection systems and network monitoring tools. They also conduct thorough incident response investigations, analysing the scope and impact of attacks, and implementing appropriate countermeasures.

**IT and Security Personnel:**
IT and security personnel collaborate with the Blue Team to deploy and maintain effective security controls, including strong encryption protocols and secure network configurations. They monitor and analyse network and system logs, reporting any suspicious activities. They also provide expertise in incident response, assisting with investigations and mitigation efforts.

**Executive Sponsor:**
The executive sponsor provides strategic guidance and support for the exercise, aligning it with the organization's cybersecurity objectives. They ensure the allocation of necessary resources, review findings and recommendations, and drive the implementation of necessary changes to enhance security defences.

## Exercise Scope and Rules of Engagement:

**Exercise Scope:**

In this engagement, teams are attempting to determine RightPoint's susceptibility to a MiTM attack. For each iteration of this exercise, teams involved must determine the specific systems, networks, or infrastructure components that will be included in the testing environment. This may include critical assets, network segments, or specific applications that are of interest for testing vulnerabilities and assessing the organization's security posture. The exercise will focus on one of the most common methods used by threat actors, that of ARP spoofing. It also requires identifying the participating team members, roles, and responsibilities involved in the exercise, ensuring everyone understands their roles, contributions, and limitations.

**Rules of Engagement:**

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. Legal and Ethical Boundaries:**
Emphasize the importance of conducting the exercise within legal and ethical frameworks. Clearly communicate that all activities must comply with applicable laws, regulations, and organizational policies. Participants must not engage in any unauthorized or malicious actions that could result in harm to systems, networks, or individuals that are not specifically included as authorised targets in the exercise.

**3. Communication Protocols:**
Define the channels and protocols for communication between the participating teams. Establish mechanisms for reporting findings, sharing intelligence, and coordinating actions. Encourage open and transparent communication while ensuring that sensitive information is appropriately handled and protected.

**4. Incident Response Procedures:**
Outline the procedures and protocols to be followed in the event of a successful MITM attack. Clearly define the steps for incident reporting, escalation processes, and coordination with the relevant stakeholders. Promptly address any identified vulnerabilities or incidents to mitigate potential risks and ensure a swift response.

**5. Data Protection and Privacy:**
Ensure the exercise respects data protection and privacy requirements. Define guidelines for handling sensitive information, including any personal or confidential data. Implement measures to anonymize or de-identify data when necessary and obtain appropriate consent or permissions for data collection and use during the exercise.

**6. Safety Precautions:**
Prioritize the safety of systems, networks, and personnel during the exercise. Implement safeguards to prevent unintended disruptions to critical services or infrastructure. Avoid actions that could result in damage, data loss, or harm to individuals or the operational

enterprise network. Adhere to any network segmentation guidelines to minimize the impact of the exercise on production environments.

**7. Post-Exercise Clean-up:**
Specify the steps and responsibilities for restoring systems and networks to their original state after the exercise concludes. Ensure that any changes or artifacts introduced during the exercise are removed or remediated properly. This includes restoring network configurations, cleaning up log files, and addressing any residual vulnerabilities or weaknesses.

## Planning and Preparation:

**Blue Team Management:**
In the planning and preparation phase of a purple team overview for a MITM exercise, it is crucial to focus on effectively managing the blue team. This involves identifying skilled members who possess expertise in incident response, network security, and system administration. Updating incident response procedures to incorporate MITM attack scenarios ensures that the blue team is well-prepared to detect and respond to such threats. Additionally, enhancing monitoring capabilities by implementing robust security tools empowers the blue team to effectively detect and mitigate MITM attacks. Providing comprehensive training and resources to the blue team equips them with the necessary skills and knowledge to effectively contribute to the exercise.

**Red Team Management:**
Managing the Red team is a vital aspect of planning and preparation for a purple team overview. Assembling a highly skilled and experienced red team specializing in penetration testing, ethical hacking, and MITM attack simulations is essential. Developing a comprehensive playbook for the red team, outlining the tactics, techniques, and tools they will utilize during the exercise, ensures a structured and effective approach. Identifying organization specific MITM attack vectors allowing the red team to tailor their simulations to the organization's unique environment. Providing the red team with the necessary resources, equipment, and permissions enables them to execute realistic and impactful MITM attack simulations.

**Coordination and Collaboration:**
Successful coordination and collaboration between the blue and red teams are critical for a productive purple team overview. Establishing regular meetings or sync points facilitates effective communication and information sharing between the teams. Clearly defining the rules of engagement, including protocols for information sharing, collaboration, and boundaries, ensures a harmonious and efficient exercise. Encouraging constructive feedback and open dialogue between the teams promotes mutual learning and knowledge transfer, allowing both teams to benefit from each other's expertise.

**Documentation and Reporting:**
Documentation and reporting play a crucial role in the planning and preparation phase of a purple team overview for a MITM exercise. Establishing a standardized format for documenting activities, observations, and findings ensures consistency and clarity. Comprehensive documentation of attack methodologies, detected vulnerabilities, and recommended mitigation strategies provides valuable insights for the organization. Compiling a detailed report summarizing the MITM exercise, including analysis of findings, key takeaways, and actionable recommendations, helps stakeholders understand the

exercise's outcomes and facilitates informed decision-making for enhancing security controls.

## Metrics and Reporting:

**MITM attack detection rate:**
This metric measures the percentage of MITM attacks successfully detected by the blue team, which consists of the defenders or security personnel. By monitoring the network and analysing network traffic, the blue team aims to identify any signs of a MITM attack. A higher detection rate indicates that the team has effective monitoring tools, detection algorithms, and alert systems in place. It demonstrates their ability to recognize and respond to ongoing attacks promptly, minimizing potential damage and unauthorized access.

**Time to detect and mitigate:**
This metric focuses on the time taken by the blue team to identify and respond to MITM attacks. It measures the efficiency and effectiveness of the team's incident response procedures. A shorter time to detect and mitigate indicates that the team has well-defined processes, skilled personnel, and appropriate technologies to rapidly identify and mitigate MITM attacks. This metric helps organizations assess their ability to minimize the duration of an attack, limiting its impact on critical systems and data.

**Vulnerability discovery:**
During a MITM attack exercise, the attackers exploit vulnerabilities in the target system or network infrastructure to carry out their attacks. This metric involves recording the number and types of vulnerabilities that were successfully exploited during the exercise. It provides valuable insights into the organization's overall security posture and identifies areas where vulnerabilities exist. By analysing the discovered vulnerabilities, organizations can prioritize their remediation efforts and strengthen their defences against potential MITM attacks in the future.

**User response rate:**
This metric evaluates the rate at which users detect and report suspicious network activities or warnings related to MITM attacks. Users play a crucial role in maintaining the security of the network by being vigilant and promptly reporting any suspicious activities. A higher user response rate indicates a higher level of user awareness and engagement with security protocols. It also helps organizations assess the effectiveness of their user awareness training programs and the success of their efforts to promote a security-conscious culture within the organization.

**Attack impact analysis:**
This metric involves assessing the potential impact of successful MITM attacks on the organization's systems, data, and operations. It helps identify the critical areas where an attack could lead to severe consequences, such as unauthorized access to sensitive systems, data exposure, or the compromise of critical assets. By analysing the potential impact, organizations can prioritize their defensive measures and allocate resources to protect the most critical assets. It also aids in identifying any gaps or weaknesses in existing security controls and implementing appropriate countermeasures to mitigate the impact of future MITM attacks.

**Executive summary:**
The executive summary provides a brief and concise overview of the MITM attack exercise. It communicates the purpose and objectives of the exercise in non-technical language that can be easily understood by executives and decision-makers. It also summarizes the key findings and highlights any significant implications or recommendations resulting from the exercise. The executive summary serves as a high-level snapshot of the exercise, enabling executives to quickly grasp the exercise's outcomes and take appropriate actions.

**Methodology:**
The methodology section of the report outlines the approach, techniques, and tools employed during the MITM attack exercise. It provides a detailed description of the steps taken to simulate the attacks, including the tools used, the attack scenarios created, and the network configurations tested. The methodology section ensures transparency and allows readers to understand the rigor and reliability of the exercise. It also helps replicate the exercise in the future or conduct further analysis based on the provided information.

**Metrics analysis:**
This section of the report delves into an in-depth analysis of the metrics collected during the MITM attack exercise. It focuses on metrics such as the MITM attack detection rate, time to detect and mitigate, vulnerability discovery, user response rate, and attack impact analysis. The analysis provides insights into the effectiveness of the organization's security measures, incident response capabilities, user awareness, and overall security posture. By interpreting and explaining the metrics, this analysis helps identify areas of strength, vulnerabilities, and opportunities for improvement.

**Vulnerability assessment:**
The vulnerability assessment section provides a comprehensive evaluation of the vulnerabilities exploited during the MITM attack exercise. It describes the vulnerabilities in detail, including their severity, potential impact on the organization's systems and data, and the recommended remediation measures. The assessment may include vulnerability scanning reports, penetration testing results, or findings from manual analysis. This section enables organizations to prioritize their efforts in addressing the identified vulnerabilities and fortifying their defences against potential MITM attacks.

**Recommendations:**
The recommendations section offers actionable suggestions based on the findings of the MITM attack exercise. It provides specific steps and measures to enhance network security controls, strengthen incident response capabilities, and improve user awareness and training. The recommendations are tailored to address the vulnerabilities and weaknesses identified during the exercise. They serve as a roadmap for organizations to improve their security posture and mitigate the risk of MITM attacks. Each recommendation should be clear, practical, and supported by the findings and analysis presented in the report.

**Lessons learned:**
This section summarizes the key lessons learned from the MITM attack exercise. It highlights both the successes and areas requiring further attention or improvement. Lessons learned may include insights into the effectiveness of existing security controls, the impact of user awareness programs, the importance of incident response readiness, or the effectiveness of specific detection and mitigation techniques. By reflecting on these lessons, organizations can refine their security strategies, policies, and procedures to better defend against MITM attacks in the future.

# Password Cracking Attempts

With a focus on addressing password brute force attacks, this playbook outlines protective measures, such as strong password policies, regular training sessions, and safe learning environments. By implementing the playbook's strategies, RightPoint can enhance incident response capabilities, cultivate cybersecurity awareness, and safeguard their valuable assets in today's dynamic threat landscape.

## Roles and Responsibilities:

**1. Purple Team Lead:**
The Purple Team Lead plays a critical role in overseeing the entire password brute force cracking attack exercise. They facilitate communication and collaboration between the Red and Blue Teams, ensuring a cohesive approach towards achieving the exercise objectives. The Purple Team Lead defines the scope of the exercise, aligning it with organizational goals, and provides valuable feedback and guidance to both teams. They evaluate the effectiveness of the exercise, identifying areas for improvement and ensuring that the exercise contributes to enhancing the organization's overall security posture.

**2. Red Team:**
The Red Team is responsible for executing the password brute force cracking attacks to assess the organization's password security measures. Their role involves utilizing various tools and techniques, such as dictionary attacks and brute force attacks, to systematically crack passwords. The Red Team identifies weaknesses in password policies, encryption algorithms, and password storage methods. They report their findings to the Purple Team Lead and collaborate with the Blue Team to develop strategies for mitigating vulnerabilities and strengthening defences.

**3. Blue Team:**
The Blue Team is tasked with monitoring, detecting, and defending against the password brute force cracking attacks. They utilize security systems and monitoring tools to identify suspicious login attempts and patterns indicative of password cracking attempts. The Blue Team promptly responds to detected attacks, investigates compromised accounts, and implements measures to contain and mitigate the impact. They collaborate closely with the Red Team to understand their attack techniques and develop proactive defence strategies. The Blue Team also identifies and patches vulnerabilities in password security, authentication mechanisms, and account lockout policies.

**4. IT and Security Personnel:**
IT and security personnel play a crucial role in supporting the overall password brute force cracking attack exercise. They implement and enforce strong password policies, including complexity requirements and account lockout settings. IT and security personnel ensure secure configurations of systems, network devices, and authentication services to minimize the risk of password cracking attacks. They continuously monitor system logs, network traffic, and security event logs for signs of brute force cracking attempts. In collaboration with the Blue Team, they provide technical expertise and support during incident response and remediation efforts.

**5. Executive Sponsor:**
The executive sponsor provides leadership, support, and strategic guidance for the password brute force cracking attack exercise. They allocate necessary resources, including budget, personnel, and technologies, to support the exercise. The executive sponsor reviews and approves policies related to password security, incident response, and vulnerability management based on the exercise findings. They actively promote cybersecurity awareness within the organization and advocate for initiatives to strengthen password security. The executive sponsor plays a vital role in making informed decisions based on the exercise findings and recommendations to improve the organization's overall security posture.

## Exercise Scope and Rules of Engagement:

### Exercise Scope:

The password brute force attack exercise is designed to evaluate the organization's resilience against unauthorized access attempts through systematic password guessing. It encompasses a comprehensive assessment of all relevant systems, accounts, and authentication mechanisms within the organization. The exercise aims to identify vulnerabilities in password security measures, assess the effectiveness of existing authentication controls, and provide insights to enhance the organization's overall defence against password brute force attacks.

### Rules of Engagement:

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. Authorized Systems and Accounts:**
The password brute force attack exercise will exclusively target authorized systems and accounts that have been agreed upon in advance. Any unauthorized systems, accounts, or sensitive data are strictly off-limits and should not be accessed or targeted during the exercise. This ensures a focused evaluation of password security measures while maintaining the integrity and security of the organization's infrastructure.

**3. Safety and Impact:**
To prevent any unintended consequences or disruptions, the exercise will be conducted in a controlled and isolated environment separate from live systems and data. The primary objective is to simulate password brute force attacks without causing actual harm, disruption, or unauthorized access to sensitive information. Safety precautions are in place to safeguard the organization's operations and ensure the exercise is conducted without negative impacts.

**4. Collaboration and Communication:**
Effective collaboration and open communication between teams are highly encouraged throughout the exercise. Teams should actively share relevant information, insights, and findings to facilitate a comprehensive evaluation. By fostering a collaborative environment,

teams can work together to identify and address vulnerabilities, enhance defensive measures, and collectively improve the organization's resilience against password brute force attacks.

**5. Legal and Ethical Boundaries:**
The password brute force attack exercise will be conducted within legal and ethical boundaries, adhering to applicable laws, regulations, and organizational policies. Teams must conduct themselves responsibly and avoid engaging in any activities that could cause harm, violate legal regulations, or compromise ethical principles. The exercise aims to improve security practices while ensuring compliance and upholding ethical standards.

**6. Incident Response and Remediation:**
The Blue Team, responsible for defending against the simulated attacks, should promptly respond to detected password brute force attempts. They should follow established incident response procedures to mitigate the impact, investigate compromised accounts, and implement necessary remediation measures. All teams are accountable for addressing vulnerabilities and collaborating to ensure timely remediation actions are taken.

**7. Documentation and Reporting:**
Thorough documentation is essential during the exercise. Teams should meticulously record attack scenarios, findings, vulnerabilities identified, and any recommended actions. A comprehensive report will be generated at the conclusion of the exercise, summarizing the exercise's progress, outcomes, and actionable recommendations. This report will be shared with relevant stakeholders to facilitate informed decision-making and drive improvements in password security practices.

**8. Professional Conduct:**
Professionalism, respect, and integrity are expected from all participants throughout the exercise. Activities should be conducted in a constructive manner, focusing on the objectives of the exercise, and promoting a positive learning outcomes and analysis. By maintaining a professional conduct, teams can effectively work together, share knowledge, and collectively enhance the organization's security posture.

**9. Confidentiality and Data Privacy:**
Participants must uphold strict confidentiality and adhere to data privacy regulations. Any data, information, or findings obtained during the exercise by red team members must only be shared with authorized personnel on a need-to-know basis. The exercise maintains the privacy and security of organizational data and ensures that sensitive information remains protected throughout the evaluation process.

## Planning and Preparation:

**1. Objectives and Goals:**
In the planning and preparation phase, the objectives and goals of the password brute force exercise are clearly defined. The purpose is to assess the organization's resilience against password cracking attacks, identify vulnerabilities in password security measures, and

enhance the overall defence posture. The goals may include evaluating the effectiveness of password policies, testing the strength of authentication mechanisms, and measuring the incident response capabilities of the Blue Team. Clear alignment of objectives and goals ensures that the exercise is focused and meaningful.

**2. Team Composition and Roles:**
During the planning phase, the composition of the Blue and Red Teams is determined. The Blue Team, responsible for defending against the simulated attacks, consists of skilled IT and security personnel who possess expertise in incident response and vulnerability management. The Red Team, on the other hand, comprises experienced ethical hackers who specialize in executing password brute force attacks and identifying weaknesses in the organization's defences. Roles and responsibilities within each team are defined, ensuring clarity and effective coordination throughout the exercise.

**3. Communication and Collaboration:**
Effective communication and collaboration between the Blue and Red Teams are crucial for the success of the password brute force exercise. Regular meetings, briefings, and debriefings are scheduled to foster a collaborative environment. The teams share information, insights, attack methodologies, and mitigation strategies to facilitate knowledge transfer and collective learning. Collaborative tools and platforms may be utilized to streamline communication and ensure efficient collaboration between team members.

**4. Scenario Development:**
Scenarios for the password brute force exercise are carefully crafted during the planning phase. These scenarios simulate various attack vectors, including dictionary attacks, brute force attacks, and targeted attacks, to comprehensively evaluate the organization's password security measures. The scenarios are designed to replicate real-world situations while considering the specific context and challenges faced by the organization. Well-designed scenarios provide meaningful challenges for the Red Team and realistic simulations for the Blue Team to test their defences.

**5. Resources and Infrastructure:**
Adequate resources and infrastructure are allocated and prepared to support the password brute force exercise. This includes dedicated systems, virtualized environments, necessary hardware and software tools, and network configurations that mirror the organization's production environment. The resources and infrastructure should be properly set up, ensuring compatibility and availability throughout the exercise. Contingency plans and backup systems may be put in place to address any unforeseen issues that may arise.

## Metrics and Reporting:

**1. Password Complexity Analysis:**
One of the key metrics in a password cracking brute force attack exercise is the analysis of password complexity. This metric measures the strength of passwords within the organization by evaluating factors such as length, character diversity, and the presence of common patterns or easily guessable information. By assessing password complexity, the organization can identify weak passwords that are susceptible to brute force attacks and develop targeted strategies for password policy enhancements and user education.

**2. Time-to-Crack Metrics:**
Time-to-crack metrics measure the average time required to crack passwords during the exercise. This information provides insight into whether existing password security measures and the resilience of the organization's systems against brute force attacks. Time-to-crack data can be analysed in relation to factors such as password length, complexity, and the presence of additional security controls like account lockouts or multi-factor authentication. This analysis helps in understanding the feasibility of password cracking attempts and provides valuable information for strengthening password defences.

**3. Success Rate:**
The success rate metric determines the percentage of cracked passwords during the brute force attack exercise. It quantifies the effectiveness of the Red Team's password cracking techniques and highlights vulnerabilities in the organization's password security measures. By tracking the success rate, the organization can identify areas where passwords are more susceptible to cracking and implement necessary improvements to bolster password security.

**4. Incident Response Metrics:**
Incident response metrics focus on the Blue Team's ability to detect, respond to, and mitigate the impact of the password cracking brute force attacks. These metrics include mean time to detect (MTTD), mean time to respond (MTTR), and mean time to mitigate (MTTM). MTTD measures the average time taken to identify the password cracking attempts, while MTTR quantifies the average time needed to respond and contain the incident. MTTM assesses the average duration required to fully mitigate the impact of the successful password cracking attempts. These metrics provide insights into the organization's incident response capabilities and help identify areas for improvement in detecting and responding to password cracking attempts.

**5. Reporting and Documentation:**
Comprehensive reporting and documentation are crucial for the password cracking brute force attack exercise. A detailed report is prepared at the conclusion of the exercise, capturing the objectives, methodologies, findings, and recommendations. The report includes an analysis of the collected metrics, presenting a clear overview of the organization's password security vulnerabilities and the effectiveness of current password defence mechanisms. It highlights weaknesses, identifies trends, and provides actionable recommendations to enhance password security controls and overall resilience against brute force attacks. The report serves as a valuable reference for decision-makers, guiding the implementation of improvements in password policies, user education, and technical defences.

# DoS Attacks

## Introduction:

In today's digital landscape, threats like Denial of Service (DoS) attacks pose significant risks to a business’s ability to operate. This playbook will help teams understand the detrimental impact of DoS attacks on RightPoint, and effective strategies to protect against such threats. Additionally, we will explore the importance of conducting regular training sessions and provide insights on how to make training safe and productive. By embracing a collaborative approach between the red (offensive) and blue (defensive) teams, RightPoint can enhance its ability to detect, mitigate, and respond to potential cyber threats. Let's embark on this journey together to fortify your organization's security defences and safeguard your valuable assets.

## Roles and Responsibilities:

**Purple Team:**
As the Purple Team, your role is crucial in overseeing and coordinating the DoS attack exercise. You will be responsible for coordinating the overall execution of the exercise, ensuring that the defined objectives and timelines are adhered to. You will facilitate effective communication and collaboration between the Red and Blue Teams, creating an environment for information sharing and feedback. Your expertise will be instrumental in analysing the effectiveness of defensive measures and response strategies. By providing guidance and support to both teams throughout the exercise, you will foster a cohesive and productive environment, contributing to the improvement of RightPoint's security defences.

**Red Team:**
red team members primary responsibility is to simulate real-world DoS attacks to evaluate RightPoint's defences. They will utilize your expertise to identify vulnerabilities and exploit them, generating accurate attack scenarios. Documenting and reporting your findings, including attack techniques and potential mitigation strategies, is essential. Collaborating closely with the blue team is critical to ensure a comprehensive evaluation of the organization's defensive measures. Their insights will be valuable in pinpointing security weaknesses and assisting in the development of effective countermeasures.

**Blue Team:**
Blue team members role is pivotal in defending against the simulated DoS attacks during the exercise. This team is responsible for implementing and maintaining appropriate security measures on RightPoint’s network. Active monitoring of network traffic and system logs will enable the swift response to signs of attack activity. Promptly mitigating the impact of incidents and restoring normal operations is crucial. Collaborating closely with the Red Team, you will gain insights into attack methodologies and work together to enhance defence strategies. By fulfilling these responsibilities, they will strengthen RightPoint's security posture and safeguard the organization's systems and data.

**IT and Security Personnel:**
The IT and security personnel's contributions are significant to the success of the DoS Attack Exercise. They will provide technical expertise and support throughout the exercise, ensuring the smooth operation of security measures. Diligent monitoring of network and system logs will help detect any anomalies or suspicious activities. Their participation in post-exercise analysis will contribute to the development of effective mitigation strategies. With their specialized knowledge and efforts, you will bolster RightPoint's overall security readiness.

**Executive Sponsor:**
The Executive Sponsors role is pivotal in supporting the DoS Attack Exercise. They will provide necessary resources and executive-level visibility for the exercise, recognizing its importance in the organization's security strategy. Reviewing and approving recommendations derived from the exercise ensures that improvements align with the organization's objectives. Fostering a culture of security awareness and accountability is essential. By promoting the exercise's significance and encouraging ongoing commitment to strengthening RightPoint's defences, they will play a vital role in the exercise's success.

## Exercise Scope and Rules of Engagement:

**Exercise Scope:**
The exercise scope encompasses the evaluation of both network-based and application-layer attacks that could potentially disrupt or degrade critical services. The exercise will simulate realistic attack scenarios to assess the effectiveness of existing security measures, incident response procedures, and the coordination between the Red and Blue Teams. The scope also includes the evaluation of communication channels, incident reporting mechanisms, and the overall effectiveness of the organization's incident response plan.

**Rules of Engagement:**

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. Authorized Targets:**
The DoS attack exercise will solely focus on authorized targets within RightPoint's infrastructure. Only systems and services explicitly designated as part of the exercise will be targeted. This ensures that the scope remains limited to predetermined assets, minimizing any unintended impact on production systems.

**3. Legal and Ethical Compliance:**
All activities conducted during the exercise must strictly adhere to legal and ethical guidelines. Participants must refrain from engaging in any actions that could cause harm, unauthorized access, data breaches, or disruptions to systems outside the exercise scope.

**4. Communication and Coordination:**
Effective communication and coordination are vital for a successful DoS attack exercise. The Purple Team Lead will serve as the central point of contact, facilitating communication between the Red and Blue Teams. All interactions and information exchanges between the teams must be channelled through the Purple Team Lead, ensuring streamlined coordination throughout the exercise.

**5. Information Sharing:**
The Red Team is responsible for sharing details of attack vectors, techniques, and tools used with the Blue Team. This includes providing necessary information to enable timely response, analysis, and mitigation efforts. Transparent and effective information sharing enhances collaboration between the teams, enabling a comprehensive evaluation of defence strategies.

**6. No Production Impact:**
Ensuring the exercise does not impact RightPoint's production systems or services is of utmost importance. Attack simulations should be conducted in a controlled environment without causing any disruptions to the organization's operations or affecting the experience of its users. This rule helps maintain the integrity of ongoing business operations.

**7. Monitoring and Reporting:**
Thorough monitoring of the exercise is crucial to gather valuable insights. The purple team Lead and designated personnel will closely monitor all activities, findings, and observations. Documentation and accurate reporting of the exercise's progress, outcomes, and lessons learned enable post-exercise analysis and improvement.

**8. Incident Response and Mitigation:**
In the event of a successful DoS attack, the blue team assumes responsibility for prompt incident response, impact mitigation, and restoration of normal operations. The exercise will evaluate the effectiveness of incident response procedures and the coordination between the Red and Blue Teams, highlighting areas for improvement in real-world scenarios.

**9. Confidentiality and Data Protection:**
Maintaining confidentiality and protecting sensitive information encountered during the exercise is paramount. All participants must handle such information with utmost care and ensure strict confidentiality. Adhering to data privacy and protection guidelines safeguards the organization's sensitive data.

## Planning and Preparation:

**Establishing Roles and Responsibilities:**
For the planning of this exercise, purple team are responsible for identifying team leaders, assigning specific tasks, and establishing the reporting structure. The blue team will be responsible for implementing and maintaining security measures, while the red team will simulate DoS attacks. By clearly delineating these roles, responsibilities, and reporting lines, the teams can work cohesively towards the common goal of evaluating and enhancing RightPoint's defences.

**Communication and Collaboration Channels:**
Effective communication and collaboration between the blue and red teams are key to a successful DoS exercise. Establishing dedicated communication channels, such as regular meetings or a shared collaboration platform, facilitates the exchange of information, progress updates, and coordination of activities. Encouraging open communication and creating a collaborative environment fosters knowledge sharing and the efficient resolution of issues that may arise during the exercise.

**Development of Attack Scenarios and Objectives:**
During the planning, the purple team, in collaboration with the red team, will develop specific attack scenarios and objectives to be simulated during the exercise. These attack scenarios should mirror real-world threats and align with RightPoint's specific security concerns. Defining clear objectives ensures that the exercise remains focused and provides measurable outcomes that can be used to evaluate the effectiveness of existing defences.

**Resource Allocation and Availability:**
Proper resource allocation and availability are crucial for the smooth execution of the DoS exercise. This includes providing the necessary infrastructure, tools, and personnel required by both the Blue and Red Teams. Ensuring the availability of testing environments, network resources, and any specialized tools required by the teams is essential for realistic simulations and accurate evaluations. Adequate resource allocation sets the stage for a comprehensive and effective exercise.

**Establishing a Timeline and Milestones:**
Setting a timeline with defined milestones is essential for effective planning and preparation. The Purple Team should establish a timeline that outlines key activities, such as the start and end dates of the exercise, milestone checkpoints, and reporting deadlines. This helps create a structured approach and ensures that the exercise progresses in a timely manner. Regular milestones enable the evaluation of progress and provide opportunities to address any potential challenges or adjustments needed during the exercise.

**Contingency Planning:**
Developing contingency plans is crucial to mitigate potential risks or unforeseen circumstances that may arise during the DoS exercise. Identifying potential challenges and

developing contingency strategies in advance ensures the teams can quickly adapt and respond if unexpected issues occur. This may include having backup systems in place, predefined escalation procedures, or alternative communication channels. Effective contingency planning helps maintain the exercise's integrity and allows for efficient problem-solving.

## Metrics and Reporting:

**Metrics Selection:**
Key metrics to consider include response time to detect and mitigate attacks, the duration of service disruptions, percentage of successful attack mitigations, and the overall impact on business operations. These metrics provide valuable insights into the organization's ability to detect, respond, and recover from DoS attacks. By tracking and analysing these metrics, the Purple Team can assess the effectiveness of existing defences, identify areas for improvement, and measure the overall resilience of RightPoint's infrastructure against DoS attacks.

**Data Collection and Analysis:**
Thorough data collection and analysis play a vital role in assessing the effectiveness of the DoS attack exercise. The purple team should collect data on attack vectors, attack durations, impact on network and application performance, and the success rate of mitigation efforts. Analysing this data allows for a comprehensive understanding of the attack techniques used, vulnerabilities exploited, and the effectiveness of countermeasures. By analysing the collected data, the purple team can derive valuable insights to enhance defence strategies, improve incident response procedures, and strengthen the overall resilience against DoS attacks.

**Reporting Structure and Frequency:**
Establishing a clear reporting structure and defining the frequency of reporting is crucial for effective communication and monitoring progress. The Purple Team should develop a standardized reporting format that includes key findings, attack details, mitigation strategies employed, and recommendations for improvement. Regular reporting intervals, such as weekly or monthly, ensure timely feedback and enable stakeholders to track the progress of the exercise. Additionally, an executive-level report should be prepared to summarize the exercise's impact, highlight vulnerabilities, and provide actionable recommendations to senior management.

**Incident Response and Mitigation:**
During the DoS attack exercise, incident response and mitigation play a critical role in evaluating the organization's ability to detect and respond to attacks. The Blue Team should demonstrate effective incident response capabilities by promptly identifying and mitigating attacks, minimizing service disruptions, and restoring normal operations. The Purple Team should closely monitor incident response activities, assess the efficiency of mitigation strategies, and provide recommendations for improving incident response procedures. Evaluating incident response and mitigation efforts ensures that RightPoint can effectively respond to real-world DoS attacks and minimize their impact.

**Lessons Learned and Continuous Improvement:**
Conducting a thorough review and analysis of the exercise is essential for capturing lessons learned and driving continuous improvement. The Purple Team should facilitate post-exercise discussions involving all relevant stakeholders, including the blue team, IT and security personnel, and executive sponsors. By collectively examining the exercise outcomes, successes, and challenges, the organization can identify vulnerabilities, weaknesses in defence strategies, and areas for improvement. Incorporating these lessons learned into future training, policy updates, and infrastructure enhancements strengthens RightPoint's ability to mitigate and respond to DoS attacks effectively.

# *SQL Injections*

## Introduction:

A significant threat RightPoint needs to address is SQL injection, which can lead to data breaches and severe consequences for the organization. To mitigate these risks, we explore preventive measures such as secure coding practices, input validation, and parameterized queries. Through regular training sessions, we aim to educate your team about potential threats and empower them to respond effectively. Our approach prioritizes ethical practices and a safe training environment. Together, we will fortify your defences against SQL injection attacks and safeguard RightPoint from cyber threats.

## Roles and Responsibilities:

**Purple Team:**
The purple team is responsible for overseeing the entire exercise and coordinating the efforts between the red Team and blue Team. They ensure that objectives are clear, facilitate communication, and provide guidance throughout the exercise. The purple team also manages the post-exercise analysis and reporting, highlighting areas for improvement and recommendations.

**Red Team:**
The red team's primary role is to simulate real-world attackers and execute SQL injection attacks. They aim to exploit vulnerabilities, test the effectiveness of existing security controls, and provide valuable insights into potential weaknesses. The red team documents their attack methodologies and findings, providing detailed reports to the purple team for analysis.

**Blue Team:**
The blue team's responsibility is to defend against the red team's attacks and mitigate the impact of SQL injection. They actively monitor and analyze the system logs, detect and respond to malicious activities, and implement defensive measures to strengthen the organization's security posture. The blue team collaborates with the purple team to share findings, propose countermeasures, and improve incident response capabilities.

**IT and Security Personnel:**
IT and security personnel play a vital role in ensuring the smooth execution of the exercise. They provide technical support, maintain the infrastructure required for testing, and assist in implementing security controls based on the purple team's recommendations. IT and security personnel actively participate in training, enhance their skills, and contribute to the overall success of the exercise.

**Executive Sponsor:**
The Executive Sponsor provides the necessary support and resources for the SQL injection attack exercise. They act as a liaison between the purple team and executive management, ensuring alignment with organizational goals and objectives. The Executive Sponsor also

reviews the exercise outcomes, considers the recommendations, and facilitates the implementation of security enhancements.

### Exercise Scope and Rules of Engagement:

**Exercise Scope:**
The exercise scope defines the systems, networks, and applications that will be included in the SQL injection attack simulation. It outlines the boundaries within which the teams can operate and conduct their activities. The scope may specify specific servers, databases, or web applications that will be targeted during the exercise. Clear delineation of the scope ensures that the exercise remains manageable and realistic while addressing the organization's critical assets and potential vulnerabilities.

**Rules of Engagement:**

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. No unauthorized actions:**
Participants must refrain from taking actions that are not explicitly authorized within the exercise scope. This includes accessing or tampering with systems or data beyond the agreed-upon scope.

**3. Respect for production environment:**
The exercise should not disrupt the organization's production environment or impact the availability and performance of critical systems.

**4. No data exfiltration:**
The exercise strictly prohibits the extraction, copying, or unauthorized transfer of any sensitive or confidential information from the organization's systems.

**5. Collaboration and communication:**
Participants are encouraged to engage in open and transparent communication. Sharing findings, insights, and attack methodologies between the Purple Team, Red Team, and Blue Team promotes a constructive learning environment.

**6. Timelines and milestones:**
The exercise should adhere to predefined timelines and milestones. This ensures efficient coordination and allows for the analysis of progress and outcomes within the designated timeframe.

## Planning and Preparation:

**Define Objectives:**
Clearly define the objectives of the SQL injection exercise. This includes identifying specific goals, desired outcomes, and areas of focus for both the blue and red teams. Aligning these objectives ensures that the exercise addresses the organization's security priorities.

**Team Composition:**
Assemble skilled individuals with relevant expertise for both the blue and red teams. The blue team should consist of knowledgeable defenders proficient in database security, web application security, and incident response. The red team should comprise experienced offensive security professionals capable of executing realistic SQL injection attacks.

**Roles and Responsibilities:**
Assign clear roles and responsibilities to team members on both sides. This includes designating team leads, incident handlers, and technical specialists. Define the decision-making hierarchy and establish effective communication channels to ensure smooth coordination between the teams.

**Scenario Development:**
Develop realistic SQL injection attack scenarios that mimic potential real-world threats faced by the organization. Craft attack vectors, payloads, and techniques to challenge the blue team's defences. The scenarios should be aligned with the exercise objectives and reflect the organization's unique environment.

**Rules of Engagement:**
Establish rules of engagement that outline the permitted actions, restrictions, and ethical guidelines for both the Blue and Red Teams. These rules should adhere to industry best practices and address any legal, compliance, or privacy considerations.

**Knowledge Sharing**:
Facilitate knowledge sharing between the blue and red teams. Encourage the red team to provide detailed reports and documentation of their attack methodologies, findings, and any novel techniques used. This information will help the blue team gain valuable insights and enhance their defensive strategies.

**Environment Setup:**
Create a controlled testing environment that mirrors the organization's production systems. Ensure that appropriate security measures are in place to protect sensitive data and prevent accidental impact on the live environment. This may involve the use of isolated networks, virtualized systems, or dedicated testing environments.

**Communication and Collaboration:**
Establish effective communication channels and mechanisms for collaboration between the blue and red teams. Regular meetings, debriefings, and progress updates help facilitate information sharing, foster a learning environment, and ensure that both teams are working together towards achieving the exercise objectives.

## Metrics and Reporting:

**Metrics Selection:**
Identify and define metrics that align with the objectives of the SQL injection attack exercise.

These metrics should provide quantitative and qualitative measurements of the exercise's outcomes, such as the number of successful SQL injection attempts, time taken to detect and respond to attacks, and the effectiveness of implemented defences. Consider using industry-standard metrics and tailor them to suit the organization's specific needs.

**Data Collection:**
Implement mechanisms to collect data during the exercise, ensuring that relevant information is captured for analysis and reporting. This includes capturing logs, incident response actions, system performance metrics, and any other data points deemed essential for evaluating the exercise's progress and outcomes.

**Analysis and Interpretation:**
Analyse the collected data to gain insights into the performance of both the blue and red teams. Evaluate the effectiveness of defensive measures, identify vulnerabilities exposed during the exercise, and assess the quality of response and mitigation strategies employed. Interpretation of data should provide actionable recommendations for enhancing security controls and improving incident response capabilities.

**Reporting Format:**
Determine the reporting format that best suits the organization's needs, considering the intended audience and the level of detail required. Reports should include a concise executive summary, key findings, metrics analysis, lessons learned, and recommendations for improvements. Clear and concise visualization techniques, such as charts, graphs, and tables, can enhance the clarity and impact of the reports.

**Stakeholder Engagement:**
Share the exercise results and reports with relevant stakeholders, including executive management, IT and security teams, and other key decision-makers. Engage in discussions and present the findings to facilitate a comprehensive understanding of the exercise outcomes and garner support for implementing recommended improvements.

**Continuous Improvement:**
Use the findings from the exercise and the subsequent reporting as a basis for continuous improvement. Collaborate with stakeholders to prioritize and implement recommended actions, addressing identified vulnerabilities, and enhancing the organization's security posture.

# Phishing

## Introduction:

Phishing attacks pose a significant risk to RightPoint and can lead to compromised data, breached confidentiality, and damaged trust. This playbook equips the organization’s management with strategies to protect against phishing, while emphasizing regular training sessions for improved cyber awareness. By embracing the purple team approach, RIghtPoint staff will collaborate to identify vulnerabilities, test security measures, and develop robust defenses, ensuring RightPoint's resilience in the face of evolving threats and maintaining the trust of clients and partners. Let's embark on this journey towards a more secure future together.

## Roles and Responsibilities:

**Purple Team:**
The Purple Team serves as the overall coordinator and facilitator of the purple team exercises. They are responsible for managing the collaboration between the red and blue teams, overseeing the planning and execution of the exercises, and ensuring that objectives are met. The purple team lead also coordinates communication, tracks progress, and provides guidance throughout the process.

**Red Team:**
The red team comprises skilled cybersecurity professionals who emulate real-world attackers. Their primary responsibility is to simulate various cyber threats, including sophisticated phishing attacks, to assess the organization's security defenses. The red team identifies vulnerabilities, exploits weaknesses, and attempts to breach the system's security controls. They provide valuable insights into potential risks and weaknesses that need to be addressed.

**Blue Team:**
The blue team consists of internal security professionals responsible for defending RightPoint's systems and infrastructure. They actively monitor, detect, and respond to the attacks initiated by the red team. The blue team analyzes and investigates security incidents, implements defensive measures, and strengthens the organization's security posture based on the insights gained from the purple team exercises. Their role is to ensure the prompt identification and mitigation of threats, as well as the enhancement of incident response capabilities.

**IT and Security Personnel:**
This group includes the IT and security professionals who actively support the purple team exercises. They collaborate with the purple team Lead, Red Team, and Blue Team to provide technical expertise, assist in configuring security tools, and ensure the smooth integration of the exercises into the organization's infrastructure. Their responsibilities also encompass monitoring the network for any anomalous activities and responding promptly to emerging threats.

**Executive Sponsor:**
An executive sponsor from within RightPoint's leadership team plays a crucial role in supporting and championing the purple team exercises. The executive sponsor provides necessary resources, communicates the importance of the exercises to the organization, and ensures alignment with strategic objectives. They actively participate in reviewing and approving recommendations derived from the exercises, ultimately driving a culture of cybersecurity awareness and resilience throughout the organization.

## Scope and Rules of Engagement:

### Scope:

This Activity involves identifying the specific systems, networks, and user accounts that will be subject to simulated phishing attacks. The exercise scope also includes determining the phishing attack scenarios to be used, which may involve various techniques such as email spoofing, social engineering, or malicious attachments. Clear rules of engagement are established to define the permissible actions and activities during the exercise, ensuring that it is conducted ethically and within legal boundaries. Additionally, the scope considers environmental factors, such as the production or test environment, to minimize any potential impact on business operations.

### Rules of Engagement:

**1. Non-Disclosure Agreement (NDA):**
All participants involved in the purple team exercises, including the red and blue teams, IT and security personnel, and executive sponsors, must sign a non-disclosure agreement to protect sensitive information and maintain confidentiality.

**2. Conducting the Exercise Ethically and Legally:**
During the phishing exercise, it is imperative to abide by ethical and legal considerations. Unauthorized access, manipulation, or disruption of systems, networks, or data is strictly prohibited. The exercise should be carried out in compliance with all applicable laws, regulations, and organizational policies. Any actions taken during the exercise must prioritize the security and integrity of the systems and respect user privacy.

**3. Respecting User Awareness and Sensitivities:**
The phishing exercise should be designed to enhance user awareness and response without causing unnecessary alarm or distress. Phishing emails and scenarios should be crafted carefully to simulate real-world attacks while avoiding content that may be deemed offensive, discriminatory, or excessively threatening. Sensitivity to employee concerns and emotions is crucial to maintain a positive learning environment throughout the exercise.

**4. Prioritizing User Safety and Well-being:**
The safety and well-being of employees participating in the phishing exercise should be a top priority. Phishing emails and related content should not induce stress, anxiety, or fear beyond what is necessary for the exercise's objectives. Clear communication should be established, emphasizing that the exercise is a learning opportunity and that no adverse consequences will result from falling victim to a simulated phishing attack.

**5. Protecting Sensitive Information:**
Throughout the phishing exercise, the confidentiality and security of sensitive information must be maintained. Personal and sensitive data should not be collected, transmitted, or stored without proper consent and security measures. Any data collected during the exercise should be handled in accordance with privacy regulations and organizational data protection policies.

**6. Reporting and Incident Response:**
Employees should be educated on how to report suspicious emails effectively and promptly. Clear channels for reporting should be established, ensuring that employees can report incidents without hesitation or fear of reprisal. The incident response process should be well-defined, allowing for timely analysis, mitigation, and resolution of reported phishing incidents. Regular communication regarding the exercise progress and reporting expectations should be provided to all participants.

## Planning and Preparation:

### Blue Team Preparation:

To ensure an effective response to simulated phishing attacks, thorough preparation of the blue team is essential. This involves identifying key team members responsible for monitoring, detecting, and responding to phishing incidents. Equipping the blue team with appropriate tools, technologies, and resources such as email filters, sandbox environments, and threat intelligence feeds enhances their ability to analyze phishing emails. Conducting training sessions on phishing techniques, indicators of phishing attempts, and incident response procedures further strengthens the Blue Team's preparedness. Clearly defining roles and responsibilities within the team, including incident reporting and mitigation, ensures a coordinated and efficient response.

### Red Team Preparation:

Proper preparation of the red team, responsible for simulating the phishing attacks, is crucial. This includes selecting skilled individuals with experience in crafting realistic and sophisticated phishing scenarios. Developing diverse attack vectors, including social engineering techniques, email spoofing, and malicious payloads, ensures a comprehensive assessment. Collaborating with the Blue Team to establish rules of engagement and facilitate information sharing fosters a constructive working relationship. Coordination between the Red and Blue Teams is essential for maintaining the exercise's integrity and achieving the desired objectives.

### Scenario Design and Execution:

Designing and executing realistic phishing attack scenarios is paramount for an effective exercise. This involves creating phishing emails that closely resemble real-world attacks in terms of sender addresses, content, and formatting. Tailoring the attack scenarios to the organization's industry, internal policies, and common threat vectors ensures relevance. Sending the red team's phishing emails to a representative sample of user accounts across different roles and departments within the organization provides a comprehensive assessment. Proper scheduling and coordination of the exercise minimizes disruptions to business operations while maximizing its impact.

**Communication and Coordination:**
Effective communication and coordination between the blue and red teams are vital throughout the exercise. Establishing clear lines of communication enables incident reporting, analysis, and feedback. Pre-exercise briefings align both teams on objectives, rules of engagement, and timelines. Ongoing communication addresses challenges, provides real-time updates, and fosters a collaborative environment. Encouraging open dialogue and knowledge sharing enhances mutual understanding and facilitates a coordinated response. Strong communication and coordination between the teams contribute to the exercise's overall success.

## Metrics and Reporting:

**Metric Selection:**
Selecting the appropriate metrics is crucial to effectively assess the outcomes of the phishing exercise. Consider metrics such as the Phishing Email Open Rate, Click-Through Rate (CTR), Awareness Improvement, Incident Response Time, User Reporting Rate, and Remediation Time. These metrics provide insights into user behaviour, incident response efficiency, and the overall impact of the exercise. By carefully choosing relevant metrics, organizations can measure the success of their phishing exercise and identify areas for improvement in cybersecurity defences.

**Data Collection:**
Establishing a systematic approach to data collection is essential for capturing relevant information during the phishing exercise. This involves leveraging security tools, phishing simulation platforms, and manual reporting channels to collect data automatically and manually. By utilizing these methods, organizations can gather data on metrics such as email gateway logs, endpoint protection systems, user behaviour analytics, and user-reported incidents. Collecting both quantitative and qualitative data enables a comprehensive understanding of the exercise outcomes and facilitates insightful analysis.

**Reporting and Analysis:**
Regular reporting and analysis of the collected data provide valuable insights and actionable recommendations. The reports should highlight key metrics, trends, and observations, presenting them in a clear and understandable format with visual aids such as charts and graphs. Analysing the data helps identify patterns, vulnerabilities, and areas for improvement in user awareness, incident response, and overall cybersecurity defences. Comparing the results with baseline measurements or industry benchmarks provides context and allows for an assessment of the organization's performance. Based on the findings, organizations can provide actionable recommendations to enhance training, awareness programs, and security controls.

**Continuous Improvement:**
The metrics and reporting from the phishing exercise serve as a foundation for continuous improvement. Regular reviews of the metrics allow organizations to track progress over time and identify long-term trends. By leveraging the insights gained, organizations can enhance employee training and awareness programs, focusing on areas where vulnerabilities were identified. Sharing the findings and recommendations with relevant stakeholders fosters a culture of cybersecurity awareness and collaboration. Incorporating the lessons learned into

future phishing exercises refines the scenarios, improves incident response, and measures the effectiveness of implemented security controls. Continuous improvement based on metrics and reporting strengthens the organization's resilience against phishing threats.

By implementing a comprehensive metrics and reporting framework, organizations can evaluate the outcomes of their phishing exercise, identify areas for improvement, and enhance their overall cybersecurity posture. Careful selection of metrics, systematic data collection, insightful reporting and analysis, and a commitment to continuous improvement contribute to building a robust defence against phishing attacks.