MINDGARD

The Complete Red Teaming Checklist

Development

Establish the foundation of the red teaming exercise, including roles, responsibilities, and methodologies.

- [ ] Define the scope of the red teaming exercise (systems, assets, and objectives)
- [ ] Identify key stakeholders, including IT, security teams, and executives
- [ ] Assemble the red team, ensuring necessary expertise in cyber, physical, and social engineering threats
- [ ] Assign roles and responsibilities to team members (leader, penetration testers, social engineers, etc.)
- [ ] Establish communication protocols between the red, blue, and purple teams
- [ ] Define Tactics, Techniques, and Procedures (TTPs) to be used
- [ ] Ensure compliance with legal and ethical guidelines
- [ ] Develop templates for:
  - [ ] Rules of Engagement (RoE)
  - [ ] Technical briefings
  - [ ] Reporting structures
  - [ ] Incident documentation
- [ ] Set up infrastructure for attack simulations (C2 servers, testing environments, etc.)
- [ ] Conduct a risk assessment to determine potential adverse impacts
- [ ] Secure executive sponsorship to ensure buy-in and support

Planning

Define operational guidelines, methodologies, and constraints before execution.

- [ ] Develop and document the Rules of Engagement (RoE):
  - [ ] Approved attack techniques
  - [ ] Systems that are off-limits
  - [ ] Allowed exploitation depth
  - [ ] Communication protocols during testing

Planning

- [ ] Set clear goals for the red team (e.g., test network security, evaluate employee phishing awareness)
- [ ] Conduct target reconnaissance, including:
  - [ ] OSINT (Open-Source Intelligence) gathering
  - [ ] Domain and IP enumeration
  - [ ] Employee social media research
  - [ ] External attack surface analysis
- [ ] Identify attack vectors (cyber, physical, and social engineering)
- [ ] Define an escalation plan in case a real security issue arises
- [ ] Align red teaming efforts with compliance requirements (ISO 27001, NIST, GDPR, etc.)
- [ ] Predefine incident response protocols if unintended disruptions occur
- [ ] Develop attack scenarios, including:
  - [ ] Credential theft and lateral movement
  - [ ] Phishing campaigns
  - [ ] Physical access attempts
  - [ ] Insider threat simulation
- [ ] Review and approve all plans with security leadership before execution

Execution

Simulate real-world attacks while maintaining detailed documentation of all actions.

- [ ] Conduct an initial team briefing to ensure alignment
- [ ] Begin executing the attack plan, capturing detailed logs and evidence
- [ ] Use various attack techniques, including:
  - [ ] Spear phishing and credential harvesting
  - [ ] Network penetration testing
  - [ ] Application and API security testing
  - [ ] Social engineering (phone calls, impersonation, baiting)
  - [ ] Physical security breaches (tailgating, lock picking)
- [ ] Maintain real-time logs of:
  - [ ] Actions taken
  - [ ] Systems compromised
  - [ ] Screenshots and artifacts collected
- [ ] Regularly meet (e.g., twice daily) to discuss findings and adjust tactics
- [ ] Communicate critical security gaps to a predefined contact if necessary
- [ ] Ensure operational continuity is maintained—avoid disrupting business functions

Execution

- [ ] Use attack simulation tools (e.g., Mindgard)
- [ ] If a real security gap is identified, document it and notify responsible teams
- [ ] Adhere strictly to the RoE and halt testing if business continuity is at risk

Reporting & Mitigation

Document findings and develop actionable recommendations for remediation.

- [ ] Conduct an internal red team debrief to review findings and insights
- [ ] Generate a comprehensive report, including:
  - [ ] Exploited vulnerabilities
  - [ ] Attack methodologies used
  - [ ] Impact assessment
  - [ ] Screenshots, logs, and evidence
  - [ ] Recommendations for mitigation
- [ ] Present findings to leadership, security teams, and relevant stakeholders
- [ ] Conduct a cross-team review with blue and purple teams to validate findings
- [ ] Prioritize vulnerabilities based on severity and exploitability
- [ ] Develop a remediation roadmap with assigned responsibilities and deadlines
- [ ] Ensure that security gaps are documented for compliance and future reference
- [ ] Collaborate with the blue team to test remediation efforts
- [ ] Implement quick fixes where possible and track progress over time
- [ ] Ensure leadership accountability for implementing security improvements

Continuous Improvement & Feedback Loops

Ensure ongoing enhancement of red teaming processes.

- [ ] Conduct post-exercise debriefs with red and blue teams
- [ ] Identify lessons learned and areas for improvement
- [ ] Update rules of engagement (RoE) based on insights gained
- [ ] Refine attack methodologies and expand the scope of future red teaming exercises
- [ ] Train red team members on emerging threats and new attack techniques
- [ ] Schedule follow-up testing to validate mitigation efforts
- [ ] Automate parts of red teaming efforts using AI-driven security validation
- [ ] Keep up with evolving threat landscapes, including AI-based attacks
- [ ] Ensure compliance with new regulatory and industry standards
- [ ] Maintain cross-team collaboration to integrate red teaming insights into long-term security strategies