Red Team Scoping Questionnaire

The red team scoping questionnaire serves as a guide for red team assessments. It helps red team planners conduct thorough scoping meetings with clients. The planner uses a structured approach to gather essential information about the client's infrastructure, objectives, and constraints.

Scoping Questionnaire

Red Team Defined

- Red Teaming is a process that simulates real-world threats using tactics, techniques, and procedures (TTPs).
- Primary goals are:
  - Measuring the effectiveness of an organization's defense mechanisms.
  - Assessing personnel in defensive strategies.
- Red Teaming does not prioritize:
  - Hunting for vulnerabilities, flaws, or bugs.
- Instead, it aims to:
  - Evaluate overall security operations (people, processes, and technology).
  - Provide insights into the defensive security posture.
  - Assess the impact of red team activities.

Purpose of Red Teaming

- Evaluate the organization's security posture holistically, including:
  - People: phishing, physical social eng., impersonation.
  - Processes: incident response, policy adherence, business processes.
  - Technology: network IDS, IPS, EDR, FW, gateway, physical controls, web proxy.
- Test specific threat scenarios to:
  - Identify strengths in defensive activities.
  - Pinpoint weaknesses in security measures.
  - Provide defenders with a safe, controlled environment to understand threat actions.
- Offer risk-free experience against adversarial threats by:
  - Simulating attacks using tactics employed by real cyber threats.
  - Targeting the same assets and information that actual attackers would pursue.

Scoping

1. What are the key reasons for performing the assessment?

Certification	Accreditation	Exercise
Cyber Hygiene	Assess Sensor Emplacement	Incident Response Procedures

2. What are you trying to achieve by performing the assessment?
3. List any milestones/tasks you would like to accomplish.
4. Timeline (Start and End Date) project completion date.

Mission Scoping Questions

Define the parameters, constraints, and objectives that shape the assessment. This scoping process establishes the boundaries of the engagement while determining the specific requirements for personnel allocation, equipment procurement, tool selection, authorized activities, and necessary training programs.

- What are your organization's capabilities? (e.g., a medium-sized financial services firm with internal IT and security teams)
- What networks are in scope? (e.g., corporate network and customer-facing web applications)
- What is the classification of the networks? (e.g., unclassified, sensitive financial data, private, proprietary, public)
- What is the size of the networks? (e.g., 500 endpoints and 50 servers)
- How geographically dispersed? (e.g., main office in New York, with smaller branches in Chicago and Los Angeles)
- Where is the assessment taking place? (e.g., remote assessment with physical access to New York office)
- What is the network's starting point? (e.g., external, no initial access provided, assumed breach, internal)
- Are there any systems considered out of scope? (e.g., employee personal devices, third-party cloud services, systems, IP's)
- What open-source research do you permit/limit? (e.g., all publicly available information)
- What activities are you permitted to perform? (e.g., network scanning, social engineering, phishing campaigns, exploitation of discovered vulnerabilities)
- What types of activities do you prohibit? (e.g., denial of service attacks, data exfiltration limitations: PII, HIPPA)
- What other cyber teams are participating?
- Who owns the equipment/network? (e.g., all target systems owned by the client organization, 3rd party, contracted)
- What is the duration of the assessment? (e.g., four-week, three-month engagement)

Attack Scoping Objectives

These objectives should be carefully designed to test the full spectrum of security controls and incident response procedures. When clients are uncertain about their specific needs, it's beneficial

to present them with detailed examples of common attack scenarios that align with real-world threats.

- **Data Exfiltration** (e.g., exfiltrate customer financial records from the corporate database to an external FTP server)
- **Unauthorized Software Installation** (e.g., install a key-logger on a customer service representative's workstation)
- **Phishing** (e.g., spoofed email from "IT Support" to employees requesting password resets)
- **Domain/Network Domination** (e.g., gain domain admin privileges and deploy malware across workstations)
- **Activity Sanitization** (e.g., delete security logs on compromised servers to cover tracks)
- **Access Server Authentication** (e.g., test for weak authentication on the customer-facing web application servers)
- **Defense Evasion** (e.g., use obfuscated PowerShell scripts to bypass antivirus detection)
- **Social Engineering** (e.g., impersonate a vendor to gain physical access to their New York office)
- **Privilege Escalation** (e.g., exploit a vulnerability in a legacy application to gain admin rights)
- **Information Collection** (e.g., perform OSINT gathering on key executives using social media profiles)
- **Denial of Service** (e.g., launch a DoS attack on the public-facing website during peak business hours)
- **Persistence** (e.g., create a backdoor account on the domain controller for continued access)
- **Evaluate Incident Response Procedures** (e.g., trigger a malware alert to assess the SOC team's response time and procedures)
- **Internal/External Scanning** (e.g., conduct port scans of the internal network from a compromised workstation)
- **Unauthorized system access** (e.g., brute force SSH credentials on an exposed development server)

Threat Actors

Identify threat actors relevant to your assessment goals. Research adversary groups that have targeted similar organizations and used attack methods matching your test requirements. Evaluate their tactics, motivations, and capabilities to select actors whose patterns will best inform your security assessment.

Type	Purpose	Threat Actors Examples
Intellectual Property Theft	Organizations steal valuable information to gain an advantage over their competitors.	APT41 Winnti Group, Lazarus Group - N. Korea, Cobalt Group
Supply Chain Attacks	To compromise trusted software vendors or suppliers to gain widespread access to multiple downstream customers through a single breach point.	APT29 Cozy Bear, APT17 Axiom, Agrius Iran

Extortion	To leverage stolen data or system access for financial gain through ransom demands, often combining traditional cybercrime with state-sponsored operations.	Gamaredon Aqua Blizzard, APT41 Alloy Taurus, ChamelGang CamoFei, FIN7, Carbanak
Espionage	The goal is to gather sensitive intelligence, state secrets, and strategic information from government agencies, defense contractors, and critical infrastructure to gain a political or military advantage.	APT29 Cozy Bear, APT37 ScarCruft, APT33 Holmium, CopyKittens
Insider Threats	Exploiting legitimate organizational access to steal data, sabotage systems, or grant unauthorized access to outside threat actors.	Unit 61398, disgruntled employee
Hacktivist	Political or ideological agendas are often advanced using data leaks and system disruptions to raise public awareness or embarrass targets.	APT28 Fancy Bear, Careto The Mask, Gelsemium

Defined Scoping Objectives

Specific, measurable goals established by the client that define what they aim to achieve through the red team engagement. The objectives should align with the organization's broader security strategy while remaining achievable within the engagement's constraints.

1.

2.

3.

Assessment Scoping Type (Red Team, Penetration, Vulnerability)

Specific method and scope of the assessment that defines the engagement parameters and depth of testing. Each type offers deeper levels of analysis and real-world attack emulation, allowing organizations to evaluate their security posture through complex and realistic scenarios.

External Network Test

- Scans
  - OSINT

Internal Network Test

- Sub-nets (Class B/C) to be scanned
- Number of physical locations
- Assumed breach/VPN info
- Domains

Web Application Test

- Technologies (.asp, .jsp, .php)

Social Engineering

- Phishing campaigns

- Phone calls
- Social media

Close Access Team (Physical)

- Access personnel, information, facilities
- Support insider threat program
- Support to operation security
    - Lock picking, RFID cloning

Wireless

- Number of access points
- Number of SSIDs in scope
- Number of buildings
- Rogue device checks
- Site survey

Model Type & Scoping Purpose

Full Engagement Model	• Red Team starts with no prior access, simulating an external threat. • Performs reconnaissance, identifies entry points, and gains network access. • Escalates privileges, moves laterally, and achieves objectives undetected. • Tests perimeter defenses, detection, and incident response.
Assumed Breach Model	• Red Team receives initial access, simulating a pre-existing breach. • Post-exploitation is the focus, including privilege escalation, lateral movement, data exfiltration, and persistence. • The tests focus on detecting, containing, and responding to an ongoing attack.
Custom Model	• Tailored to the organization's needs. • Combines elements of Full Engagement and Assumed Breach or focuses on specific threats. • Simulates specific attack groups, web application security, or industrial control systems. • Define scope and success criteria with the client.

Client Infrastructure Scoping - Networks, Circuits, Buildings

Inventory of in-scope assets including physical and digital infrastructure. This covers network topology, IP ranges, critical systems, applications, databases, data centers, branch offices, and remote facilities. Also includes network segment connections, cloud services, and remote access points that affect the assessment.

1.

2.

3.

Assessment Scope Accounts (Valid User, White Card, Admin, Student)

Pre-configured accounts with different access levels provided to the red team. These range from basic user accounts to administrative ones, plus test accounts for specific scenarios. Teams use

these to test insider threats, security controls, and detection capabilities across permission levels. This enables assessment of privilege management, activity monitoring, and access control systems.

1.

2.

3.

Communications

Reporting Procedures

Is the trusted agent the main point of contact for incident reporting, de-confliction?

Hot Wash debrief will be provided on what date?

Final assessment report will be provided 30 days after the assessment, on what date?

Contacts

The contacts section lists key personnel involved in the assessment, including red team leads, blue team members, management, and trusted agent/stakeholders. Contact details include names, titles, phone numbers, and email.

Name:

Phone:

Email:

Restricted Actions

Identify any activities that are off-limits such as personnel, data-exfiltration, web-sites, networks, systems, time-frame or restrictions.

1.

2.

3.

Roles Defined

This section helps planners define and explain specific roles to the customer during assessment scoping.

Red Team (Cyber Exploitation)

Purpose: The process of using tactics, techniques, and procedures to simulate a real-world threat with the goals of measuring and training the effectiveness of the people, processes, and technology used to defend the organization.

How:

- Emulate adversary threat operations.
- Perform passive & active reconnaissance to exploit systems/ application to gain unauthorized access into the network.
- Laterally move, collect & ex-filtrate, manipulate information, evade defenses, privilege escalation.

Close Access Team (CAT) – Physical, Wireless

Purpose: Conducts assessments to support the red team evaluating the organization's physical security posture, demonstrating the ability for outsiders to access organizational systems and evaluate OPSEC processes, policies, and procedures.

- OPSEC is protecting friendly information, which includes individual pieces of data that, if grouped together, would give the threat a better perspective. OPSEC protects organizational critical information.

How:

- Keep people, resources, buildings, and activities safe from threats. Is also used to support red team assessments.
- Supports insider threat program and operation security.
- Conduct passive and active wireless security assessments in support of red team operations.
- Methods consist of:
  - Wireless Password Cracking, Wi-Fi Protected Setup attacks
  - Rogue and soft access point attacks, Evil Twin Attacks, Man-in-the-Middle attacks, AP attacks, denial of service attacks, and site surveys.

Techniques:

- **Open-source research (OSINT)** – collecting public information.
- **Dumpster diving** – search through trash for valuable information.
- **Surveillance** – targeted observations.
- **Elicitation** – people prompting to reveal information.
- **Social engineering** – manipulate people to perform actions.
- **False credentialing & forgery** – copy and create badges, cards, tokens.
- **Covert access methods** - techniques used to gain entry unnoticed.
- **Enable cyber exploitation** – support red team operations.

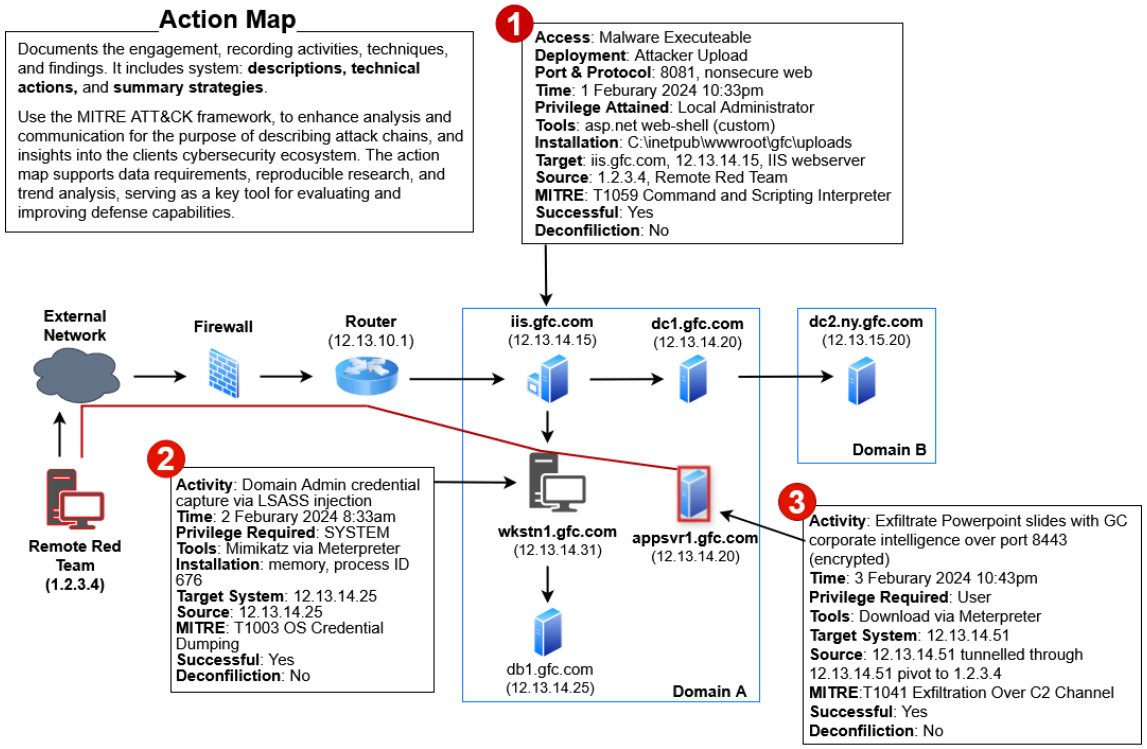
Effect Examples

Red team engagements simulate real-world cyber threats to test an organization's security. These attacks evaluate detection systems, incident response, threat identification capabilities, and security control effectiveness across multiple vectors. Through realistic scenarios, organizations can assess their defenses and find areas to strengthen. Below is a summarized effects table to help scope the assessment.

Type	Description	Target System	Expected Results	Risk	Impact	Range
Deceive	Impersonate unit leadership via communications channels; inject false messages / guidance	VOIP, Text, Chat	Org executes false commands perceived to be from leadership		Medium	Targeted Users/systems
Deceive	Phishing email with malicious attachment or link	Email	Obtain user credentials or system infection		Low	Targeted Users/systems
Deceive	Modify critical document (pdf, word, text, web-page)	User workstations and/or critical systems	Org executes false commands perceived to be from leadership	Operations impacted related to incident response	Medium	Targeted Users/systems
Degrade	Display scrolling banner at top of target system screen with Red Team message	User workstations and/or critical systems	Disrupt users and reinforce cyber awareness		Low	Targeted Users/systems
Degrade	Display pop-up box with Red Team message	User workstations and/or critical systems	Disrupt users and reinforce cyber awareness		Low	Targeted Users/systems
Degrade	Play sounds / music on target systems	User workstations and/or critical Systems	Disrupt users and reinforce cyber awareness		Low	Targeted Users/systems
Deny	Shutdown / restart of one or more critical infrastructure (once or repeated)	Critical Infra. (Domain Controller, SharePoint, File Share, Database, Exchange, Application)	Org denied use of services	Loss of data during shutdown	High	Entire Org
Deny	Change system IP address of one or more critical infrastructure	Critical Infra. (Domain Controller, SharePoint, File Share, Database, Exchange, Application)	Org denied use of services		High	Targeted Users/systems
Deny	Print red team message / spool blank paper	Printers	Disrupt users and reinforce cyber awareness		Low	Targeted Users/systems
Disrupt	Traffic injection, MitM attack	VOIP, Text, Chat	Disrupt use of Org communications and force use of a backup plan		High	Entire Org
Disrupt	Lockout System Administrator Accounts	System administrator accounts	System Administrators are unable to manage the network		Low	Targeted Users/systems
Disrupt	Lockout User Accounts	User Accounts	Deny targeted users use of network		Low	Targeted Users/systems
Disrupt	Restart target system	User workstations and/or critical systems	Disrupt users and reinforce cyber awareness	Loss of data during shutdown	Low	Targeted Users/systems

Action Map

A strategic communication tool that visually maps red team activities, objectives, and scenarios. The map aligns client expectations, identifies focus areas, and surfaces potential concerns early. While useful for scoping, it primarily serves as a post-assessment visualization of red team operations.



Notes