Adversary Emulation Engagement

Planning Template

# Instructions

The purpose of this document is to record information needed to successfully plan and execute an adversary emulation project. Go over each of these sections with the network owner(s) and record their responses.

# Disclaimer

**Please have this document reviewed by your legal counsel prior to using it for your own purposes.**

# Project Contact Information:

Who is the primary contact for this project?

|  |
| --- |
| Name:  Title:  Organization:  Phone number:  Email: |

# Objectives

What are your goals for the project (*i.e., why do you want threat emulation? What do you want to achieve?*)

Help the network owner articulate clear project objectives; consider asking leading questions such as:

* What are your cybersecurity concerns?
* What cyber threats are you most worried about?

|  |
| --- |
|  |

# Schedule

When do you want the engagement? Please provide dates (can be tentative if needed).

|  |
| --- |
|  |

During what hours should adversary emulation activities occur (9:00 AM – 5:00 PM? Time zone?)

|  |
| --- |
|  |

Are there any periods in which testing should absolutely not occur (blackout periods, maintenance, etc.)?

|  |
| --- |
|  |

# Location

Will the engagement occur on-site or remotely?

If on-site, please provide the address.

|  |
| --- |
|  |

# Approving Authorities

Please provide the contact information for the network owner(s). This should be somebody with authority to authorize this engagement. This individual will be asked to sign a permission memo authorizing the engagement.

Also be aware of approvals required by third parties, such as cloud providers (AWS, Azure, etc.). Consult with the third parties to understand their security testing approval process.

|  |
| --- |
| Name:  Title:  Organization:  Phone number:  Email: |

# Scope

Describe the target network (approximate number of devices, purpose of network(s), common operating systems and software, security products in use, etc.).

Ask for network diagrams if applicable.

|  |
| --- |
|  |

What specific devices and/or user accounts are in scope for this engagement? Please list usernames, IP addresses, subnets, hostnames, etc.

|  |
| --- |
|  |

Are there any sensitive or critical systems that should be explicitly out of scope?

|  |
| --- |
|  |

How will the adversary emulation team access the target network? Will they try to access the network via external attack? Will they be provided initial access as in an “*assumed breach*” engagement?

|  |
| --- |
|  |

# Rules of Engagement

## Techniques in Scope

As part of this threat emulation engagement, the red team will execute cyber tactics, techniques, and procedures in based on <actor/threat you will emulate>.

Detailed information about this actor’s TTP’s can be found at the following links:

* ATT&CK group page, for example: [MITRE ATT&CK - APT29](https://attack.mitre.org/groups/G0016/)
* ATT&CK Navigator page, for example: [ATT&CK Navigator - APT29](https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json)

## Red Team Accountability

Red team will maintain detailed logs with timestamps of their activity to aid in tracking and deconfliction of their activities.

Red team will maintain a list of cleanup activities to restore the network to its pre-engagement state.

As a best practice, red team does not perform destructive attacks or make irreversible changes to target systems (unless specifically requested to do so).

## Securing Customer Data

All engagement data will be encrypted in transit and at rest using strong cryptography (usually AES-256 or similar solution).

All customer data on red team systems will be wiped in accordance with NIST 800-88 following the conclusion of the engagement.

## Handling Sensitive Situations

The red team will notify the project owner(s) in any of the following circumstances:

* Credential and PII obtainment and exposure
* Detection of cohabitation of malware / threat actors
* Departure from outlined scope
* Unintended effects such as breaking a service or system
* Detection of anything unlawful observed on the network

# Communications Plan

Describe how you will communicate with the network owners to include who you will speak with, communication methods (phone call, video conference), and call frequency (daily, weekly, etc.).

**Daily meeting with project owner(s)**

|  |
| --- |
| Red team will have a daily meeting with the project owner. This will be a 15-to-30-minute meeting in which red team explains what they accomplished that day, as well as their plans for the following day. This meeting provides an essential communications channel to ensure that all stakeholders are aware of red team activities and answer any questions or concerns. |

**Routine Communications**

|  |
| --- |
| Red team will provide project stakeholders a video conference meeting for real time communications throughout the engagement. |

**Emergency Communications**

|  |
| --- |
| In the event of emergency, Red team will contact the network owner via cell phone. |

## Call Roster

List all relevant project members with their contact information. This should contain the network owners, red team, blue team, system administrators, and anyone else relevant to the project.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Title | Organization | Phone Number | Email | Remarks |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Project Deliverables

What deliverables are the project owners expecting?

Red team typically provides the following deliverables resulting from an engagement:

1. Presentation summarizing engagement activities with recommendations
2. Detailed technical report describing the project, red team activities, findings, and recommendations.

Additional deliverables such as adversary emulation plans, tools, and training may be available depending on the needs of the project.

|  |
| --- |
|  |

# Other Remarks

Document anything else that may be relevant.

|  |
| --- |
|  |