Cheatography

Red Teaming part I. Cheat Sheet

by Geringonça (akirasett) via cheatography.com/185306/cs/39024/

Nº1 Objective when Red Teaming:

Meet the client's expectations.

Main Sources

TryHackMe
RedTeam.Guide

Red Team Checklists

Source2

Campaign Planning

Engagement Plan	CONOPS, Resource and Personnel Requirements, Timelines
Operations Plan	Goes deeper into each Engagement Plan topic.
MissionsPlan	Execution time, Commands to run, Time Objectives, Responsible Operator, etc.
Remediation Plan	What to do after the engagement is done: reports, remendiation consultation, etc...

Remediation Plan

Optional plan that contains a summary of the engagement details and a report of findings,
States how the client can fix vulnerabilities.
May be included in the final report.

Mission Plan includes:

Optional Command Playbooks which include the exact commands, and tools to run including when, why and how we use them. Usefull for bigger teams.
Execution Times that state when to start each engagement stage. Timestamps and may also include commands and tools.
Roles and Responsabilities of each red team cell

Operations Plan includes:

Information on employee requirements.
Stopping conditions: How and Why
Optional RoE
Technical Requirements Necessary knowledge

Engagement Plan includes:

CONOPS & Resource Plan *(Timelines and required information to assure Red Team success)*
e.g.: Personnel, hardware, software, cloud requirements, etc..

Standart RoE Structure (acc. to TryHackMe)

1. **Executive Summary** (Contents and Authorization)
2. **Purpose** (of the RoE)
3. **References** -> ISO's, etc...
4. **Scope** -> Restrictions and Guidelines
5. **Definitions** -> Terminology
6. **Rules of Engagement and Support Agreement**
7. **Provisions** -> Adicional Info and Exceptions
8. **Requirements, Restrictions, and Authority** -> Red Cell's Expectations
9. **Ground Rules** -> Red Cell's limitations
10. **Resolution of Issues/Points of Contact**
11. **Authorizatio**n - Signatures
12. **Approval**
13. **Appendix**

Source

CONOPS Critical Components

Client Name;
Service Provider;
Timeframe;
General Objectives/Phases;
Other Training Objectives (Exfiltration);
High-Level Tools/Techniques planned to be used;
Threat group to emulate (if any).

RoE

Rules of Engagement

Vulnerability

A *weakness* in an asset or group of assets.
Can be exploited and harmed by one or more threats

Threat

Possible unwanted event.
When a threat turns into an actual event it may cause an unwanted incident.

PII

Personal Identification Information

TTS

Tactics, Techniques and Procedures

CONOPS

Concept of Operations
How to target the client and meet his expectations.

White Card

A simulated event in an operational test.
Used when a system is too fragile or operationally critical for the adversarial team to pursue an exploitation, or when the adversarial team is unable to penetrate the system, but there is still a desire to evaluate the ability of the system to react to a penetration.
Should be used only when necessary.