RED TEAM OPERATIONS & DOCUMENTATION

1. Introduction to Red Team Operations

Red Team Operations focus on the **planning, execution methodology, documentation discipline, and tracking mechanisms** used during a security assessment. Unlike a security assessment report, which highlights technical findings, Red Team documentation demonstrates how offensive security activities are organized, controlled, and reported in a professional and ethical manner.

This section documents the operational workflow, attack techniques, task tracking, and governance mechanisms followed during the Red Team engagement.

2. Rules of Engagement (RoE)

2.1 Purpose of RoE

Rules of Engagement define the **scope, permissions, and limitations** of a Red Team exercise. They ensure that all activities are conducted ethically, legally, and without unintended impact on real-world systems.

2.2 Scope Definition

In-Scope Assets

- Metasploitable2 Virtual Machine
- Kali Linux Attacker Machine

Out-of-Scope Assets

- Host Operating System
- Internet-facing or production systems
- Any third-party infrastructure

2.3 Allowed Activities

- Network scanning and enumeration
- Vulnerability assessment
- Exploitation of known vulnerabilities
- Post-exploitation and persistence simulation
- Malware detection testing using safe test files

2.4 Restricted Activities

- Denial-of-Service attacks
- Data destruction or modification
- Exploitation of real-world systems
- Installation of real malware

2.5 Ethical Statement

All activities were conducted strictly for **academic and training purposes** in an isolated lab environment. No real data or systems were harmed during the engagement.

3. Technique Summary

3.1 Exploit Documented

VSFTPD 2.3.4 Compromised Backdoor Exploit

3.2 Red Team Technique Description

The VSFTPD 2.3.4 backdoor vulnerability was exploited to gain unauthorized access to the target system. The exploit leveraged a maliciously modified FTP service that spawns a backdoor upon authentication attempts. A command shell payload was delivered, resulting in root-level access.

3.3 Red Team Terminology Used

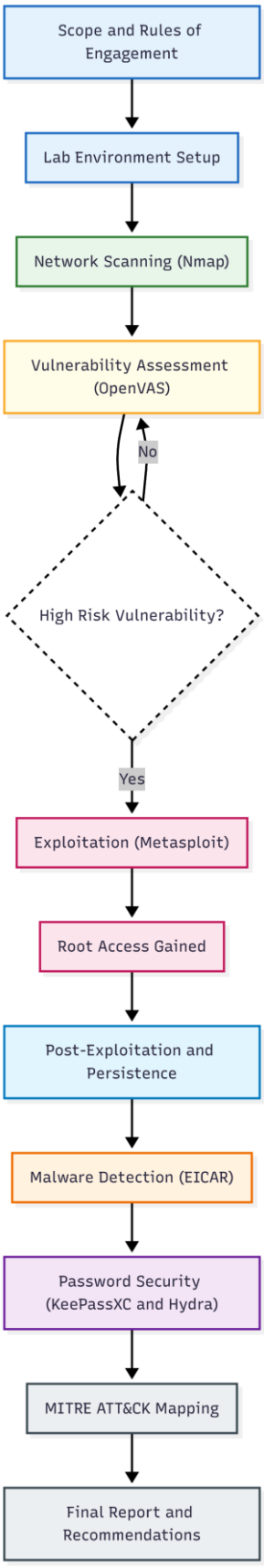
- **Exploit** – Leveraged a known vulnerability in VSFTPD
- **Payload** – Command shell payload
- **Access** – Unauthorized root-level shell access
- **Persistence** – Ability to maintain access after compromise
- **Impact** – Complete system compromise

4. Attack Flowchart Documentation

4.1 Purpose

An attack flowchart was created to visually represent the **end-to-end Red Team attack lifecycle**, from initial reconnaissance to reporting and remediation.

4.2 Attack Flow Description: The attack followed a structured Red Team methodology

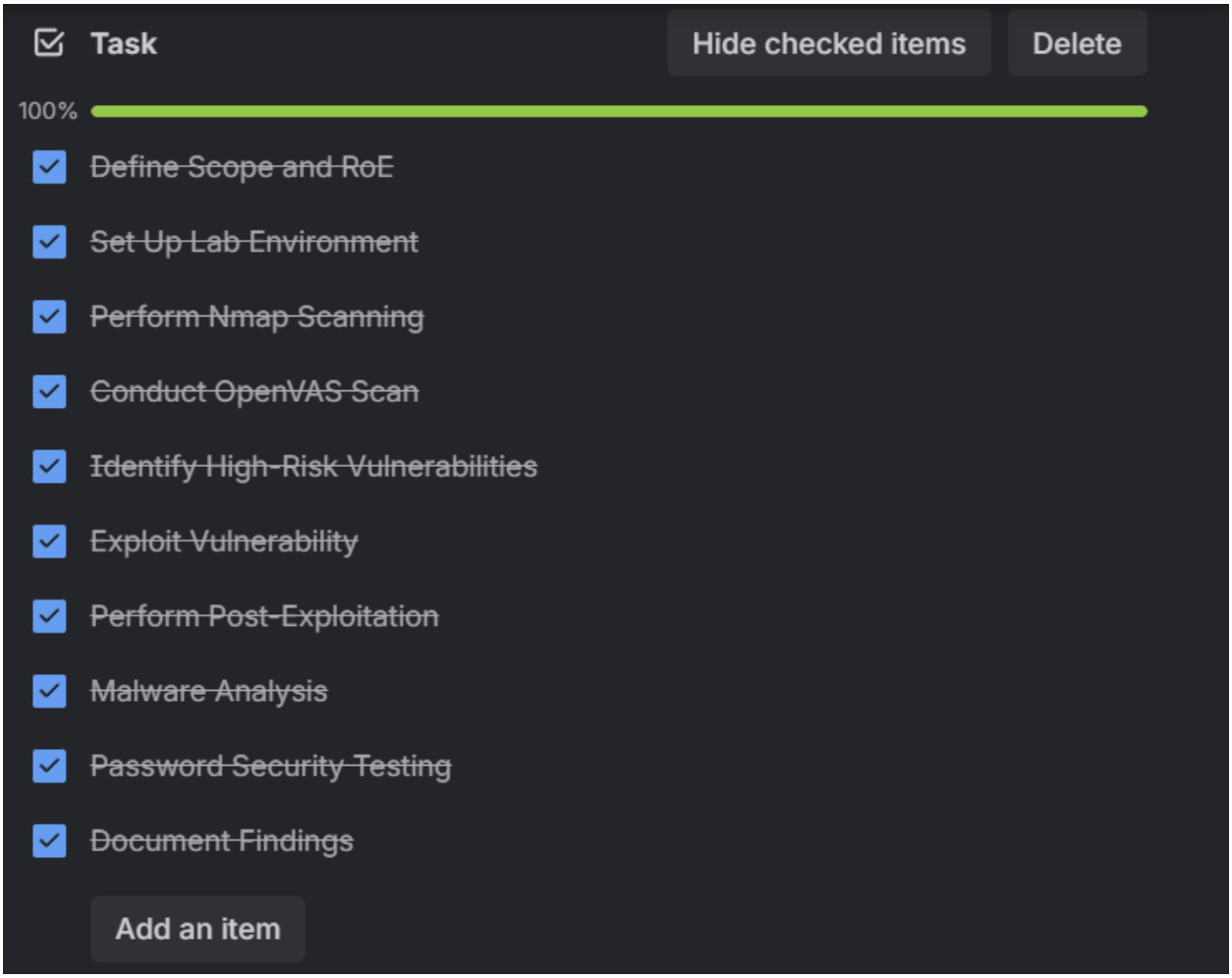

Scope and Rules of Engagement
Lab Environment Setup
Network Scanning (Nmap)
Vulnerability Assessment (OpenVAS)
No
High Risk Vulnerability?
Yes
Exploitation (Metasploit)
Root Access Gained
Post-Exploitation and Persistence
Malware Detection (EICAR)
Password Security (KeePassXC and Hydra)
MITRE ATT&CK Mapping
Final Report and Recommendations

5. Red Team Checklist (Task Tracking – Trello)

5.1 Purpose of Checklist

A Red Team checklist ensures **methodical execution and accountability** throughout the engagement. It helps track completed tasks and prevents missed steps during assessments.

5.2 Red Team Checklist Items



6. MITRE ATT&CK Mapping

6.1 Technique Identified

- **T1059 – Command and Scripting Interpreter**

6.2 Mapping Summary

The exploitation activity maps to MITRE ATT&CK technique T1059, as the attacker gained command execution through a remote shell after exploiting the VSFTPD backdoor. This technique enables adversaries to execute arbitrary commands, perform post-exploitation activities, and establish persistent access on compromised systems.

7. Documentation and Reporting Practices

Throughout the engagement, all findings, commands, outputs, and screenshots were documented systematically. Technical findings were recorded in the Security Assessment Report, while operational workflows, planning artifacts, and tracking mechanisms were documented in this Red Team Operations section.

This separation ensures clarity between **technical impact** and **operational methodology**.

8. Red Team Operations Summary

This Red Team Operations and Documentation exercise demonstrated a structured, ethical, and professional approach to offensive security assessments. The use of defined rules of engagement, attack documentation, flowcharts, and task tracking reflects real-world Red Team practices. Proper documentation enhances accountability, reproducibility, and communication with stakeholders.