NISA-book

Network Information Security Association

2024-12-13

Table of contents

Preface

This is a Quarto book.

To learn more about Quarto books visit https://quarto.org/docs/books.

1 Introduction

This is a book created from markdown and executable code.

> See Knuth (1984) for additional discussion of literate programming.

2 Summary

In summary, this book has no content whatsoever.

Part I

Penetration - 渗透测试

3 介绍

渗透测试

3.1 渗透流程

按照 The Cyber Kill Chain 的相关设计，渗透测试分为以下七个步骤

3.1.1 Reconnaissance - 侦察

Reconnaissance 是网络杀伤链的第一阶段，涉及在进行任何渗透测试之前研究潜在目标。侦察阶段可能包括识别潜在目标、发现其漏洞、发现哪些第三方与其连接（以及他们可以访问哪些数据）、探索现有入口点以及寻找新入口点。侦察可以在线和离线进行。

3.1.2 Weaponization - 武器化

网络杀伤链的 Weaponization 阶段发生在侦察发生并且攻击者发现有关潜在目标的所有必要信息（例如漏洞）之后。在武器化阶段，攻击者的所有准备工作最终都会创建用于针对已识别目标的恶意软件。武器化可以包括创建新型恶意软件或修改现有工具以用于网络攻击。例如，网络犯罪分子可能会对现有勒索软件变体进行细微修改，以创建新的网络杀伤链工具。

3.1.3 Delivery - 交付

在 Delivery 阶段，网络武器和其他网络杀伤链工具用于渗透目标网络并接触用户。传递可能涉及包含恶意软件附件的网络钓鱼电子邮件，其主题行会提示用户点击。交付还可以采取侵入组织网络并利用硬件或软件漏洞渗透的形式。

3.1.4 Exploitation - 执行

Exploitation 是交付和武器化之后的阶段。在网络杀伤链的利用步骤中，攻击者利用他们在前一阶段发现的漏洞进一步渗透目标网络并实现其目标。在此过程中，网络犯罪分子通常会在网络中横向移动以达到他们的目标。如果网络负责人没有部署欺骗措施，利用有时可能会将攻击者引向目标。

3.1.5 Installation - 部署

在网络犯罪分子利用目标的漏洞获取网络访问权限后，他们开始网络杀伤链的 `Installation` 阶段：尝试将恶意软件和其他网络武器安装到目标网络上，以控制其系统并窃取有价值的数据。在此步骤中，网络犯罪分子可能会使用特洛伊木马、后门或命令行界面安装网络武器和恶意软件。

3.1.6 Command and Control- 命令与控制

在网络杀伤链的 `Command and Control` 阶段，网络犯罪分子与他们安装到目标网络上的恶意软件进行通信，以指示网络武器或工具来实现其目标。例如，攻击者可能使用通信渠道引导感染 `Mirai` 僵尸网络恶意软件的计算机使网站流量过载，或使用 C2 服务器指示计算机执行网络犯罪目标。

3.1.7 Actions on Objectives - 行动与目标

网络犯罪分子开发出网络武器，将其安装到目标网络并控制目标网络后，他们开始网络杀伤链的最后阶段：实现网络攻击目标。虽然网络犯罪分子的目标因网络攻击的类型而异，但一些示例包括将僵尸网络武器化以通过分布式拒绝服务 (DDoS) 攻击中断服务、分发恶意软件以窃取目标组织的敏感数据以及使用勒索软件进行网络勒索工具。

References

Knuth, Donald E. 1984. "Literate Programming." *Comput. J.* 27 (2): 97–111. https://doi.org/10.1093/comjnl/27.2.97.