项目 1

Web 安全实验环境搭建

项目导读

随着数字化时代的到来，网络安全不仅成为国家稳定发展的重要保障，也成为国家安全的重要组成部分。全面认识网络安全，提高网络安全意识，采取网络安全防范措施，对保障网络安全乃至国家安全都有着重要的意义。

当前，网络安全形势严峻，威胁手段不断演变，这对网络安全提出了更高的要求。尽管许多安全措施和协议已被业界广泛采用，如 HTTPS、SSL/TLS 加密、内容安全策略（CSP）等，但 Web 应用程序和服务仍面临着诸多安全威胁，这些威胁包括跨站脚本攻击（XSS）、SQL 注入、DDoS 攻击、数据泄露等。企业和开发者必须采取更为严格的安全策略和持续的监控措施，以确保用户数据的安全和服务的稳定运行。此外，随着新技术的出现，如云计算、物联网（internet of things，IoT）和人工智能（artificial intelligence，AI），Web 安全领域也在不断演变，需要新的安全解决方案来应对更加复杂的挑战。

开发人员在开发 Web 应用程序时一定使用过无数的开源库，但是开发人员是否自己确认过这些库可以安全使用？它们更新了吗？这些库中是否存在漏洞？它们是否定期维护？这些都是开发人员在使用这些开源库时需要思考的问题，因为这些库中只需出现单个可利用的漏洞就会导致开发的 Web 应用程序受到攻击的风险大大增加。例如，攻击者可能会以 Log4J 等广泛使用的库为目标，去利用和危害数百万个 Web 应用程序。此类威胁背后的原因在于，有时开发人员或系统管理员甚至可能不知道 Web 应用程序中正在使用哪些库。

随着人工智能技术的不断进步，攻击者也在尝试利用这些技术来实施更高级、更复杂的网络攻击。例如，DeepFake 技术可以通过生成假冒的语音、视频和图像来欺骗民众，造成严重的社会影响。生成式人工智能还可能被用于创建更具欺骗性的网络钓鱼电子邮件和恶意软件，从而增加网络攻击的成功率。

对于防范这些新型网络攻击，需要采取一系列的措施。首先，需要加强人工智能技术的监管，防止其被滥用。其次，需要提高人们对人工智能技术的认识和警惕性，以便更好地识别和防范网络攻击。此外，还需要加强网络安全技术的研究和应用，以应对不断变化的网络威胁。

学习目标

- 了解 HTTP/HTTPS 协议的工作机制、Web 应用架构及各层安全风险；
- 掌握 Web 安全实验环境搭建方法；
- 掌握 HTTP 工作原理；
- 掌握 HTTP 会话技术的使用方法；
- 能够截取 HTTP/HTTPS 会话；
- 能够暴力破解 Web 登录密码。

职业能力要求

- 熟练掌握虚拟机软件和容器技术的使用，能够搭建和配置多样的操作系统环境，如 Windows、Linux 等；
- 能够安装、配置和管理 Web 服务器、数据库以及各种中间件；
- 熟悉常见的 Web 开发框架的部署与配置；
- 在搭建实验环境和进行安全测试过程中，严格遵守相关法律法规，不侵犯他人隐私，不对未授权的系统进行攻击或破坏。

职业素质目标

- 在搭建实验环境时，注意要每一个环节准确无误，如系统配置、软件安装、网络设置等，确保实验环境的真实性和有效性，能反映出真实世界中的 Web 安全问题；
- 具备独立查找资料、解决问题的能力，面对未知的 Web 安全技术和工具，能够自我研究并熟练掌握其使用方法；
- 在多人协作完成大型实验项目时，具备良好的沟通协调能力和团队合作精神，能够共同规划、分配任务，高效地完成实验环境搭建工作；
- Web 安全领域发展迅速，应养成追踪前沿技术动态的习惯，不断更新和扩展自己的知识体系，以适应不断变化的安全环境。

项目重难点

项目内容	工作任务	建议学时	技能点	重难点	重要程度
Web 安全实验环境搭建	任务 1.1　实验环境搭建	2	仿真环境的搭建	虚拟机安装	★★★☆☆
				Web 安全靶场	★★★★★
	任务 1.2　实验环境网络配置	2	虚拟网络模式的应用	虚拟网络模式应用	★★★★★
				虚拟操作系统 IP 配置	★★★★★
	任务 1.3　Pikachu 靶场实验环境搭建	2	在 LAMP 环境下运行 Web 靶场	LAMP 环境搭建	★★★☆☆
				安装 Pikachu 靶场	★★★★★

续表

项目内容	工作任务	建议学时	技 能 点	重 难 点	重要程度
Web 安全实验环境搭建	任务 1.4　模拟网络请求，理解 HTTP 工作原理	2	分析 HTTP 请求与响应过程	HTTP 请求头	★★★★★
				HTTP 响应头	★★★★★
				HTTP 请求方法	★★★★★
				HTTP 状态码	★★★★★
	任务 1.5　初识 Cookie 技术	1	分析 Cookie 在 Web 应用程序中的应用	Cookie 的工作原理	★★★☆☆
				Cookie 相关的安全问题与防范措施	★★★★★
	任务 1.6　初识 Session 技术	1	分析 Session 在 Web 应用程序中的应用	Session 的工作原理	★★★★★
				Session 相关的安全问题与防范措施	★★★★★
	任务 1.7　截取 HTTP 请求	2	使用 Burp Suite 工具截取 HTTP 会话	Burp Suite 工具使用	★★★★★
				截取 HTTP 会话	★★★★★
				截取 HTTPS 会话	★★★★★
	任务 1.8　暴力破解 Web 登录密码	2	使用 Burp Suite 工具暴力破解 Web 登录密码	暴力破解原理	★★★★★
				Intruder 模块的使用	★★★★★

任务 1.1　实验环境搭建

学习目标

知识目标：掌握虚拟化技术 VMware 和 Docker 的技术的应用。

能力目标：能够独立搭建包含多种操作系统、Web 服务器、数据库等元素的实验环境。

建议学时

2 学时

任务要求

本任务主要是搭建一个 Web 安全仿真环境，环境中包含攻击机和靶机，攻击机集成了常用的漏洞测试工具，如 Burp Suite、sqlmap、Nmap、Metasploit 等。Web 安全靶场模拟真实的网络环境，并包含大量已知的漏洞。读者在学习过程中，可利用这些漏洞进行练习，提高攻击和防御能力。

知识归纳

1. 虚拟化软件介绍

虚拟化软件是一种可以在单一物理主机上创建和运行多个虚拟环境的软件，能使每个虚拟环境都如同一台独立的计算机，拥有自己的操作系统、应用程序和资源。以下介绍几款主流虚拟化软件及其优缺点。

1）VMware vSphere/Workstation/Fusion

优点：VMware 是虚拟化市场的领导者，其产品成熟稳定，性能优越，尤其是在硬件资源的充分利用和隔离方面表现出色。vSphere 为企业级用户提供了一整套数据中心虚拟化解决方案，而 Workstation 和 Fusion 则分别对应桌面级 Windows/Linux 和 macOS 环境下的虚拟机管理。VMware 提供了丰富的高级功能，如实时迁移、高可用性集群、虚拟网络功能等。

缺点：商业版价格相对较高，免费版功能有限，占用系统资源较多，对宿主机的硬件配置有一定要求。

2）VirtualBox

优点：VirtualBox 是一款开源免费的虚拟化软件，具备跨平台支持能力，可支持 Windows、Linux、macOS、Solaris 等操作系统。它简单易用，安装和配置十分便捷，支持大量客户机操作系统，而且提供了许多高级功能，如拖放文件、无缝窗口模式等。

缺点：相较于 VMware，VirtualBox 在性能和稳定性上稍逊一筹，尤其是对于图形密集型应用和高端 I/O 负载的支持不够理想。另外，它的虚拟网络配置相比 VMware 较为复杂。

3）Hyper-V

优点：Hyper-V 是微软提供的内置虚拟化技术，免费提供给 Windows Server 和 Windows 10 Pro/Enterprise 用户使用。它与 Windows 系统的集成度极高，支持 Windows 和 Linux 等多个操作系统，具备高性能和可靠的虚拟化能力，支持 Live Migration 等企业级功能。

缺点：对于非 Windows 平台的兼容性和支持度相对较弱，且在一些高级功能上（如 GPU 虚拟化、存储复制等）可能不及 VMware vSphere。对新手来说，其管理界面不如 VMware 直观友好。

4）Docker

优点：Docker 并非传统的完全虚拟化方案，而是采用轻量级的容器技术，其资源消耗少，启动速度快，非常适合微服务架构和持续集成/持续部署（CI/CD）流程，以及开发、测试环境的快速搭建和管理。

缺点：容器相比于虚拟机隔离性较低，不适合对隔离性要求极高的场景。此外，虽然 Docker 可用于 Linux 和 Windows 应用，但在 Windows 上的表现和生态尚不如 Linux 完善。

5）KVM

优点：KVM(kernel-based virtual machine)是 Linux 内核的一部分，作为一种开源虚拟化技术，它具有很高的性能和灵活性。通过结合 libvirt 和 QEMU，KVM 可提供企业级虚拟化解决方案，尤其在大规模云服务提供方中有广泛应用。

缺点：KVM 主要面向 Linux 环境，对于非 Linux 用户的友好度不高，且管理工具链相对复杂。同时，相对于商业虚拟化产品，KVM 在某些高级特性和技术支持方面可能略显不足。

每种虚拟化软件都有各自的定位和应用场景，选择哪种虚拟化技术取决于项目具体需求，如预算、性能要求、操作系统支持、管理便捷性、业务场景等因素。

2. Kali Linux 介绍

Kali Linux 是一种专门面向网络安全专业人士和渗透测试人员设计的基于 Debian 的 Linux 发行版。Kali Linux 由 Offensive Security 团队开发、维护和资助，其诞生是为了满足高级渗透测试、安全评估和数字取证的需求。Kali Linux 继承自 BackTrack，后者在 2013 年进行了彻底重构并严格按照 Debian 开发标准进行优化，从而形成了更加稳定和兼容的 Kali Linux 系统。

Kali Linux 的一大特色在于其预装了大量的安全和渗透测试工具，数量超过 300 个，这些工具按照功能可划分为 14 类，包括但不限于网络侦查、漏洞分析、密码破解、社会工程学工具、无线攻击、逆向工程、取证分析等领域。其中包含的知名工具有 Nmap(网络扫描器)、Wireshark(网络封包分析器)、John the Ripper(密码破解工具)、Aircrack-ng(无线网络破解套件)、Metasploit Framework(渗透测试框架)和 Burp Suite(Web 应用安全测试工具)等。

Kali Linux 广泛支持各种硬件平台，提供 x86 架构的 32 位和 64 位版本，同时也支持 ARM 架构，适用于如树莓派等嵌入式设备。用户可以通过硬盘安装、Live CD 或 Live USB 等方式运行 Kali Linux，这使得它成为一个非常便携和灵活的安全测试平台。

此外，Kali Linux 的目录结构遵循 Linux 的标准布局，如/bin、/boot、/dev 等，确保用户可以根据传统的 Linux 知识轻松操作和管理系统。同时，Kali Linux 还提供了易于使用的图形界面和命令行界面，让不同的用户群体都能方便地开展工作。

Kali Linux 更新频繁，与最新安全研究和工具能够保持同步，并且注重社区参与和贡献，鼓励用户参与到项目的改进和发展中。由于其独特的专业用途，Kali Linux 在网络安全教育、企业安全评估以及个人安全研究中都扮演了重要的角色。

3. LAMP 介绍

LAMP 是一种流行的开源 Web 应用程序架构的缩写，全称为“Linux，Apache，MySQL，PHP/Perl/Python”。这一架构集合了四个开源技术栈，共同为构建和部署动态网站和 Web 应用提供高效、可靠和经济实惠的解决方案。

(1) Linux：作为操作系统层，提供了一种稳定且定制性较强的基础环境。因其所具有的开源、安全和高效的特点，Linux 成为服务器端运行 Web 服务的理想选择。常见的 Linux 发行版如 Ubuntu、CentOS、Debian 等都被广泛用于搭建 LAMP 服务器。

（2）Apache：作为 Web 服务器软件，Apache 是最流行的 HTTP 服务器之一，负责接收 HTTP 请求，解析请求内容，并将服务器上的静态和动态内容传送到客户端浏览器。Apache 支持多种模块扩展，能够处理大量并发连接，并可根据需求进行高度定制。

（3）MySQL：作为一种著名的关系数据库管理系统，它可用于存储网站的数据，如用户信息、产品目录、文章内容等。MySQL 提供高效的数据查询和事务处理能力，同时因其开源和跨平台的特性，成为 Web 应用中最常使用的后端数据库之一。

（4）PHP/Perl/Python：都是用来开发动态网页和后端逻辑的脚本语言，其中 PHP 最为典型。PHP 主要用于处理 Apache 传递过来的动态请求，生成动态内容并返回给客户端。PHP 可以直接嵌入 HTML 代码中，与 MySQL 数据库交互，实现用户登录验证、数据读写等功能。Perl 和 Python 同样可以在这个架构中承担类似的角色，为 Web 应用提供动态内容生成和业务逻辑处理。

4. LAMP 架构的优势

LAMP 架构的优势如下。

（1）成本低：所有组件均为开源的，无需支付额外许可费用。

（2）可靠稳定：经过长期的社区维护和市场检验，LAMP 组件都有较高的稳定性和可靠性。

（3）开发效率高：PHP/Perl/Python 等脚本语言开发周期短，有大量的开源库和框架可供使用。

（4）扩展性强：可根据项目需求自由组合和扩展各个组件的功能。

因此，LAMP 架构在 Web 开发领域得到了广泛应用，尤其适合中小企业和个人开发者快速搭建和部署 Web 应用。随着技术的发展，尽管现在出现了许多其他现代 Web 开发栈，但 LAMP 仍然是很多传统 Web 应用的重要基石。

任务实施

步骤 1： 下载虚拟化软件，完成安装虚拟化软件。

步骤 2： 打开浏览器，在 Kali 官方网站下载 ISO 镜像。

步骤 3： 在虚拟化软件平台中，新建虚拟机；输入虚拟机的名称 Kali，选择虚拟机存储位置，选择 Linux 虚拟操作系统、debian64 版本，内存至少 2GB，设置磁盘容量为 30GB，CPU 至少为 2 核，虚拟光驱选择 Kali 镜像文件，在虚拟机设置好之后，启动虚拟机。根据安装提示向导完成 Kali 虚拟机的安装，如图 1-1 所示。

步骤 4： 下载靶机的镜像安装包，将靶机文件解压，打开虚拟化软件，选择“文件”→“打开”命令，选择已解压后的 ovf 文件，输入新虚拟机名称和新虚拟机的存储路径，单击“导入”按钮，如图 1-2 所示。

步骤 5： 运行虚拟机，在 VMware Workstation 中，分别单击 Kali 和 Ubuntu 虚拟机，然后单击“启动”按钮，启动攻击机 Kali 如图 1-3 所示，启动靶机如图 1-4 所示。

图 1-1　Kali 攻击机基本配置

图 1-2　导入靶机的镜像安装包

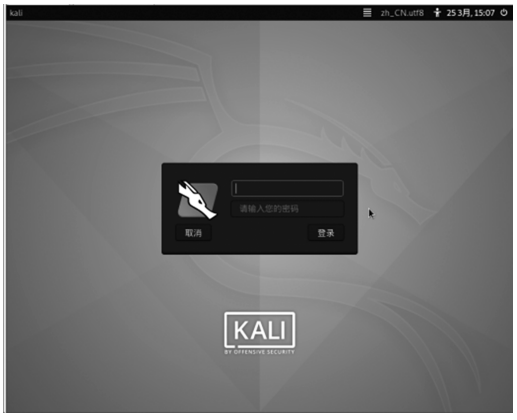

图 1-3　Kali 登录界面

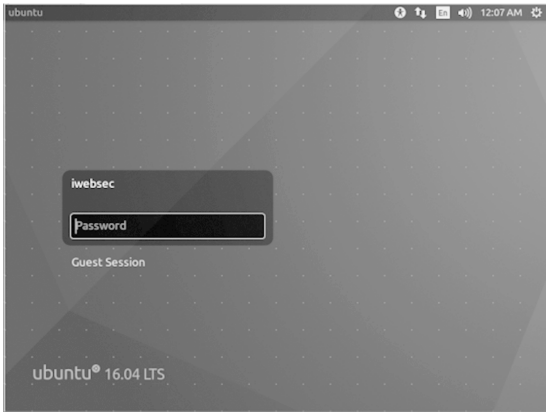

图 1-4　Ubuntu 登录界面

任务小结

本任务搭建了 Web 安全实验测试环境，选择了基于 Linux 的 Kali Linux 作为攻击端，Ubuntu Server 作为目标服务器。Kali Linux 预装了丰富的渗透测试工具，目标服务器采用 LAMP 架构，设计有多种常见安全漏洞的 Web 应用，作为实验的目标靶场。初学者通过模拟 Web 应用中常见的安全漏洞和攻击手段，深入了解 Web 应用的工作原理，以及如何进行有效的防护和修复。通过反复实验和练习，以提高自己的实践能力、应急响应能力，并为安全研究和开发工作提供有力的支持。

任务 1.2　实验环境网络配置

学习目标

知识目标：学习和理解 VMware Workstation 的网络模式，如 NAT、桥接、仅主机模式和自定义网络等，以及每种模式在网络中的作用、优缺点和适用场景。

能力目标：能够在 Kali Linux 和 Ubuntu 操作系统中手动配置网络接口，包括静态 IP 地址设置，确保虚拟机之间以及虚拟机与外部网络之间的网络连通性。

建议学时

2 学时

任务要求

VMware Workstation 使用桥接模式、网络地址转换、仅主机模式和自定义网络连接虚拟机，分别对 Kali Linux 和 Ubuntu 虚拟机分配静态 IP 地址，包括 IP 地址、子网掩码、默认网关及 DNS 服务器等信息。使用 ping 命令测试虚拟机之间的连通性。

知识归纳

1. VMware Workstation 网络连接模式

Web 安全实验环境由攻击机和靶机构成，攻击机和靶机连接到同一网络才能互相通信。虚拟机网络连接主要有三种应用模式：Bridged 模式、NAT 模式和 Host-Only 模式。

（1）在 Bridged 模式下，VMware 虚拟出来的操作系统就像是局域网中的一台独立的主机，可以访问网内任何一台机器。需要手工为虚拟系统配置 IP 地址、子网掩码和网关，而且还要和宿主机处于同一网段，这样虚拟系统才能和宿主机进行通信。

（2）使用 NAT 模式，就是让虚拟系统借助网络地址转换功能，通过宿主机所在的网络来访问公网。在 NAT 模式下，VMnet8 虚拟网络为虚拟系统提供 DHCP 服务，为虚拟系统

动态分配 IP 地址，实现在虚拟系统里访问互联网。采用 NAT 模式最大的优势是虚拟系统接入互联网非常简单，不需要进行任何其他的配置，只需要主机能访问互联网即可。

(3) 在 Host-Only 模式下，虚拟网络是一个全封闭的网络，它唯一能够访问的就是主机。其实 Host-Only 网络和 NAT 网络很相似，不同的地方就是 Host-Only 网络没有 NAT 服务，所以虚拟网络不能连接到互联网。主机和虚拟机之间的通信是通过 VMnet1 虚拟网卡来实现的，此时如果想要虚拟机访问外网则需要主机联网并且网络共享。

安装了 VMware 虚拟机后，默认会在本地网络连接中生成三块虚拟网卡。

- VMnet0：用于 Bridged 模式下的虚拟交换机。
- VMnet1：用于 Host-Only 模式下的虚拟交换机。
- VMnet8：用于 NAT 模式下的虚拟交换机。

2. Kali Linux IP 地址配置

Kali Linux 是一款专业的渗透测试和安全审计操作系统，它可以运行在物理机或虚拟机上。为了让 Kali Linux 能够与网络通信，需要配置它的 IP 地址。IP 地址配置的方法有静态配置和动态配置两种。在静态配置下，需要手动指定 IP 地址、子网掩码、网关和 DNS 服务器等信息。这样的好处是 IP 地址不会变化，方便进行网络扫描和攻击。而对于动态配置，则需要通过 DHCP 自动获取 IP 地址等信息，这样的好处是不需要手动设置，适合临时使用或者网络环境变化频繁的情况。

Kali Linux IP 地址的配置步骤如下。

(1) 打开 Kali Linux 的终端窗口，输入 ifconfig 命令查看当前的 IP 地址。

(2) 要配置静态 IP 地址，输入如下命令，打开配置文件。

```
sudo vim /etc/network/interfaces
```

(3) 在 eth0 网卡的配置中，static 是手动配置 IP 地址，将 address 设置为要配置的 IP 地址，将 netmask 设置为要配置的子网掩码，将 gateway 设置为要配置的网关。配置文件如下：

```
auto eth0
iface eth0 inet static
address 192.168.201.100
netmask 255.255.255.0
gateway 192.168.201.1
```

(4) 输入 wq，保存并退出 vim 编辑器。

(5) 输入如下命令重新启动网络服务。

```
sudo service networking restart
```

(6) 再次输入 ifconfig 命令，验证 IP 地址是否已成功配置。

注意

动态配置只需将 static 改为 dhcp，将 address、netmask 和 gateway 配置内容删除即可。

3. Ubuntu IP 地址配置

Ubuntu 是一种基于 Debian 的 Linux 操作系统，由 Canonical 公司开发和维护。Ubuntu 的目标是为个人和企业用户提供一个易用、安全、稳定和免费的桌面和服务器平台。Ubuntu 的特点包括以下几点。

(1) 每半年发布一个新版本，每两年发布一个长期支持(LTS)版本，提供 5 年的安全更新和技术支持。

(2) 使用 GNOME 作为默认的桌面环境，提供友好的用户界面和丰富的应用程序。

(3) 使用 apt 作为软件包管理器，可以方便地安装、更新和卸载软件。

(4) 支持多种硬件平台，包括 x86、x86_64、ARM 和 RISC-V。

(5) 遵循开源和自由软件的理念，鼓励用户参与社区和贡献代码。

Ubuntu 系统的 IP 地址配置与 Kali 类似，具体步骤如下。

(1) 打开 Ubuntu 的终端窗口，输入 ifconfig 命令查看当前的 IP 地址。

(2) 要配置静态 IP 地址，输入如下命令。

```
sudo vim /etc/network/interfaces
```

(3) 在 eth0 网卡的配置中，将 address 设置为要配置的 IP 地址，将 netmask 设置为要配置的子网掩码，将 gateway 设置为要配置的网关。配置文件如下：

```
auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.1
```

(4) 输入 wq，保存并退出 vim 编辑器。

(5) 输入如下命令重新启动网络。

```
sudo service networking restart
```

(6) 再次输入 ifconfig 命令，验证 IP 地址是否已成功配置。

注意

在 Kail 和 Ubuntu 操作系统图形界面的网络配置中已存在 IP 地址的配置文件，在重新启动网络服务时会造成配置冲突，因此在网络服务重新启动前应删除图形界面下的网络配置文件。

使用 ifconfig 命令查看网络配置时，会显示网卡名称，需将配置文件中的网卡名称修改为 ifconfig 查看的网卡名称。

任务实施

步骤 1： 修改 Kali 虚拟机的网络连接为“仅主机模式”，如图 1-5 所示，使用 root 用户登