项目 1

走进渗透测试技术

项目导读

在信息技术迅猛发展的当下，网络安全已成为各行各业关注的焦点。渗透测试技术，作为一种专门针对目标网络系统进行全方位安全检测和精准评估的有效手段，旨在深入挖掘网络中潜藏的漏洞和安全隐患，为相关组织机构提供切实可行的改进意见和方法，从而强化网络安全。

本项目涵盖渗透测试技术的前导内容，其中包括渗透测试技术的基本概念、执行标准、常见的渗透测试方法、技术工具及专业术语，帮助读者熟悉并掌握渗透测试的原理。同时，项目涉及的相关法律法规也会进行介绍，以确保读者在操作过程中遵纪守法。最后，我们还将强调渗透测试人员的职业素养和能力要求，帮助读者提升综合素质，成为优秀的网络安全渗透测试人员。

完成本项目的学习，读者将在渗透测试技术领域迈出坚实的第一步，并能够探索其奥秘，拓宽技术视野，从而为未来的职业发展奠定坚实的基础。

学习目标

- 理解渗透测试的基本概念及相关的法律法规；
- 熟悉渗透测试执行标准；
- 掌握渗透测试领域的常用行业术语、工具及平台。

职业素养目标

- 根据《中华人民共和国网络安全法》（以下简称《网络安全法》）等相关法律法规，不得利用渗透测试技术从事非法活动，如窃取他人信息、破坏他人系统等；在进行渗透测试前，务必获得合法授权，并确保测试过程不会对目标系统造成实质性损害；

- 严格遵守客户隐私政策，保守秘密，未经许可不得泄露敏感信息；
- 坚守良好的职业道德和品格，具备较强的自我调适能力，不断提高自身的技术水平和业务能力；
- 尊重客户、合作伙伴和其他参与者，努力构建一个公平、公正的社会环境。

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
走进渗透测试技术	任务 1.1　渗透测试的基本概念	1	定义及测试方法	分辨三种测试方法的差异及应用场景	★★★★★
	任务 1.2　渗透测试执行标准	1	各阶段的关键任务	理解各任务之间的分界线	★★★★★
	任务 1.3　渗透测试工具及平台	1	熟悉主要工具及平台	了解不同渗透测试平台的优缺点及应用场景	★★★★★
	任务 1.4　常见行业术语	1	熟悉行业术语	理解行业术语及应用场景	★★★★★

任务 1.1　渗透测试的基本概念

微课：渗透测试的基本概念

任务描述

本任务将介绍渗透测试技术的相关概念，包括渗透测试技术的定义、测试方法、测试目标及相关法律法规等。

知识归纳

1. 渗透测试的定义

渗透测试（Penetration Testing）是一种针对目标网络及相关系统进行安全检测和评估的技术，通过模拟恶意攻击者的行为，对目标系统的安全性进行测试，从而找出系统中存在的漏洞和安全弱点。渗透测试工程师通常从攻击者的角度出发，运用各种黑客技术和工具，对相关组织机构的网络基础设施、应用程序和物理安全措施等进行安全评估和测试。

2. 渗透测试的方法

根据事先对目标信息的了解程度，渗透测试分为黑盒测试、白盒测试和灰盒测试三种方法。

（1）黑盒测试（Black-Box Testing）也称为外部测试。在进行黑盒测试时，渗透测试

人员全方位模拟真实网络环境中的外部攻击者，并在对目标网络的内部结构和所使用的系统环境完全不了解的情况下，采用攻击技术与工具对其进行安全评估测试。在黑盒测试中，需要耗费大量的时间完成对目标信息的收集。除此之外，黑盒测试对渗透测试人员的要求也是最高的。这种类型的测试方法更有利于挖掘系统潜在的漏洞、薄弱环节和薄弱点等。

（2）白盒测试（White-Box Testing）也称为内部测试。在进行白盒测试时，渗透测试人员必须事先清楚被测试环境的内部结构和技术细节，这可以让渗透测试人员以最小的代价发现和验证系统中存在的严重漏洞。相较于黑盒测试，白盒测试的目标是明确定义好的，因此无须进行目标定位和信息收集等操作。渗透测试人员可以通过正常渠道从被测试单位获得需要的资料，包括网络拓扑、员工资料甚至网站程序的代码片段，也可以和单位其他员工进行面对面沟通。

白盒测试的缺点：无法有效地测试客户的应急响应程序，也无法判断他们的安全防护计划对检测特定攻击的效率。白盒测试的优点：在测试中发现和解决安全漏洞所花费的时间和代价要比黑盒测试少很多。

（3）灰盒测试（Gray-Box Testing）就是将白盒测试和黑盒测试组合使用。它可以对目标系统进行更加深入和全面的安全审查。组合的好处就是，能够同时发挥两种渗透测试方法各自的优势。在采用灰盒测试方法的外部渗透攻击场景中，渗透测试者也需要从外部逐步渗透目标网络，但他拥有的目标网络底层拓扑与架构将有助于选择更好的攻击途径与方法，从而达到更好的渗透测试效果。

3. 网络安全渗透测试的目标

网络安全渗透测试的目标包括一切和网络相关的基础设施，主要包括以下方面。

（1）网络设备：路由器、交换机、防火墙、无线接入点、服务器、办公计算机等。

（2）操作系统：Windows、Linux、UNIX 等。

（3）物理安全：数据中心、通信竖井、通信线路等。

（4）应用程序：针对某种应用目的所使用的程序，如 OA 系统、邮件系统、财务系统等。

（5）管理制度：为保证网络安全对使用者提出的要求和做出的限制。

4. 渗透测试相关的法律法规

在进行渗透测试时需要遵守的法律法规因国家和地区而异。在我国，网络安全从业人员应遵守“无授权，不渗透”这条重要原则。未经授权进行渗透测试属于非法行为，可能会被视为黑客攻击或未授权访问。渗透测试活动还应该严格遵循以下原则。

（1）授权：在测试开始之前，必须有一个正式的授权过程，通常包括签署渗透测试授权书。

（2）合规性：测试应符合当地的法律和行业规定。

（3）范围：测试的范围应该明确界定，包括哪些系统、网络和应用程序可以测试，哪些是禁止测试的。

（4）保密性：渗透测试可能会泄露敏感信息，因此必须确保所有发现的信息都得到妥善保护，并只与授权人员共享。

（5）报告：测试完成后应提供详细的报告，包括发现的漏洞、利用的方法和建议的修复措施。

5. 国内网络安全相关的政策法规

1）网络安全法律法规

（1）《网络安全法》第二十七条：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

（2）《中华人民共和国刑法》（以下简称《刑法》）第二百八十五条规定了非法侵入计算机信息系统罪。

该法条规定：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

（3）《中华人民共和国保守国家秘密法》是为保守国家秘密、维护国家安全和利益、保障改革开放和社会主义建设事业的顺利进行制定的法律。2024 年 2 月 27 日，第十四届全国人大常委会第八次会议表决通过新修订的《中华人民共和国保守国家秘密法》，并于 2024 年 5 月 1 日起施行。

（4）《中华人民共和国国家安全法》（以下简称《国家安全法》）是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定的一部法律。

2）政策条例标准

国内网络安全的政策、条例、标准有《关于加强国家网络安全标准化工作的若干意见》《中华人民共和国计算机信息系统安全保护条例》《信息安全技术—网络安全等级保护基本要求》《网络安全等级保护条例》和《网络产品和服务安全审查办法》。

根据以上法律法规与政策条例的明确规定，如果渗透测试者未经授权进行测试，就可能违反《网络安全法》和《刑法》等相关法律，根据侵害的严重程度，可能面临行政处罚或刑事责任。

（1）非法侵入计算机信息系统：根据《刑法》第二百八十五条规定，非法侵入他人计算机信息系统，情节严重者应处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。

（2）非法获取数据：非法获取、出售或者提供计算机信息系统中的数据和通信内容，若情节严重，可按照相同法条受到处罚。

（3）破坏计算机信息系统：故意破坏计算机信息系统功能、程序和数据的行为，严重危害计算机信息系统正常运行，并因此对公共利益或他人利益造成严重损害的行为，根据《刑法》的相关规定，应处三年以上七年以下有期徒刑。

任务实施

步骤 1：收集不同的渗透测试案例。

步骤 2：根据案例分析使用了哪种渗透测试方法。

步骤 3：在测试过程中应该遵循哪些相关的法律法规。

步骤 4：阅读渗透测试中违反职业道德和法律法规的案例，找出其中渗透测试的风险和责任，避免在实际工作中触碰法律底线或违背职业操守，确保测试过程的合法性和道德性。

任务 1.2　渗透测试执行标准

微课：渗透测试执行标准

任务描述

本任务将紧密围绕行业中广泛应用的渗透测试执行标准展开，深入剖析渗透测试的全过程，包括从初步的信息收集到最终的渗透报告撰写等 7 个阶段。通过本任务的深入学习与实践，读者将熟练掌握 PTES（Penetration Testing Execution Standard，渗透测试执行标准），为今后网络安全工作的开展奠定坚实的基础。

知识归纳

当前，PTES 已经成为安全行业的一项重要标准。这一标准为企业组织与安全服务提供方提供一套国际通用的描述准则，以便更加规范、有效地实施渗透测试。PTES 的广泛采纳和应用，不仅有助于提升渗透测试的专业性和准确性，更能为企业网络安全防护提供坚实的保障，强化企业信息安全。PTES 将渗透测试过程划分为 7 个阶段，分别为：前期交互、信息收集、威胁建模、漏洞分析、渗透攻击、后渗透攻击以及渗透报告。PTES 过程如图 1-1 所示。

1. 前期交互（Pre-Engagement Interaction）

在这个阶段，渗透测试团队需与客户进行深入沟通，明确渗透测试的目标、范围、测试方法、限制条件以及服务细节等内容，拟定服务合同并获取合法的渗透测试授权。该阶段通常包括以下活动：收集客户需求、准备测试计划、定义测试范围与边界、明确业务目标、进行项目管理和规划等。

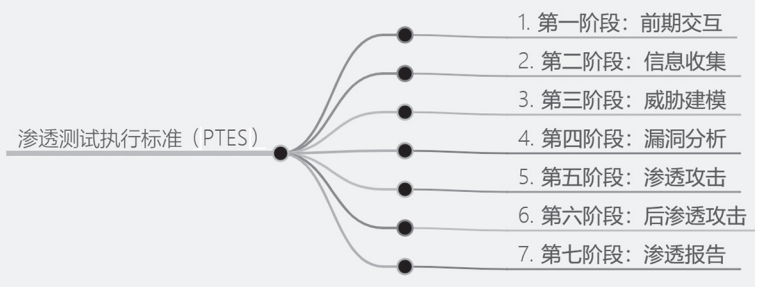

图 1-1　PTES 过程

2. 信息收集（Information Gathering）

在这个阶段，渗透测试人员需要尽可能全面地收集信息，包括使用开源情报（OSINT）、搜索引擎、资产测绘平台、社会工程学等进行信息收集，为后续的渗透测试做好准备。在这个阶段收集到的信息越充分，对之后的渗透测试越有利。

3. 威胁建模（Threat Modeling）

在这个阶段，渗透测试人员需要对收集到的信息进行整理和分析，以制订攻击规划方案及可行的攻击通道。这是渗透测试过程中非常重要但又很容易被忽略的一个阶段。在这个过程中，必须厘清思路，确定最有效、最可行的攻击方案。

4. 漏洞分析（Vulnerability Analysis）

在这个阶段，渗透测试人员需要综合前几个阶段获取的情报信息，特别是安全漏洞扫描结果和服务查点信息，通过搜索可用的渗透代码资源，找出可实施的渗透攻击点，并在测试环境中进行验证。高水平的渗透测试团队还会针对攻击通道上的关键系统和服务进行安全漏洞探测和挖掘，找出可利用的未知安全漏洞，并开发渗透代码，从而打开关键路径。

5. 渗透攻击（Exploitation）

在这个阶段，渗透测试团队需要利用发现的目标系统安全漏洞，正式入侵系统并获得访问控制权。渗透攻击可以使用公开渠道获取渗透代码，但高水平的测试者通常需要根据目标系统的特性制订攻击方案，并使目标网络和系统中的安全防御措施失效，才能成功实现渗透目标。渗透测试者还需要考虑绕过目标系统的检测机制，以避免引起目标组织中安全响应团队的警觉。

6. 后渗透攻击（Post-exploitation）

在这个阶段，渗透测试人员需要根据被测试方的安全防御特点、业务管理模式、资产保护流程等，识别被测试方的核心设备、最有价值的信息及资产，最终能够对客户组织造成最重要业务影响的攻击途径，保持可持续的控制，从而更进一步实现横向和纵向攻击。

7. 渗透报告（Reporting）

在这个阶段，渗透测试团队需要针对整个渗透测试过程以书面文档形式撰写渗透测试报告。报告中应包含目标关键情报信息、渗透测试发现的漏洞详情、成功渗透的攻击过程、造成业务影响的攻击途径，以及从安全维护角度给出的在安全防御体系中存在的薄弱

点和风险评估等，并给出专业的修复和改善建议。

任务实施

步骤 1：阅读、分析企业渗透测试案例。

步骤 2：运用 PTES 对案例中的渗透攻击路径进行讨论。

任务 1.3　渗透测试工具及平台

微课：渗透测试工具及平台

任务描述

渗透测试工具及平台能有效地助力渗透测试人员更迅速、更精准、更高效地完成渗透测试的相关工作。本任务将着重介绍几款常用的开源渗透测试工具以及集成化渗透测试平台。

知识归纳

1. 常用开源渗透测试工具

根据功能的不同，开源渗透测试工具可分为：信息收集工具、漏洞扫描与分析工具、Web 应用安全测试和攻击工具、密码破解工具、无线安全测试工具、社会工程相关工具等，如表 1-1 所示。

表 1-1　渗透测试工具汇总

工具分类	介　绍
信息收集工具	（1）Nmap：用于网络映射和安全审核的工具，可以探测目标网络的活动主机、开放端口、运行的服务版本等 （2）Shodan：互联网搜索引擎，可以搜索全球范围内的设备，如服务器、网络摄像头、打印机等 （3）Maltego：用于开源情报收集和数据关系分析的图形化工具
漏洞扫描与分析工具	（1）Nessus：商业漏洞扫描工具，用于检测网络中的安全漏洞 （2）OpenVAS：开源漏洞评估系统，用来扫描服务器和网络设备中的安全风险 （3）Burp Suite：一个集成化的平台，提供多种工具来执行对 Web 应用程序的安全测试
Web 应用安全测试和攻击工具	（1）OWASP ZAP（Zed Attack Proxy）：针对 Web 应用程序的渗透测试工具，帮助发现应用中的安全漏洞 （2）SQLmap：自动化检测和利用 SQL 注入漏洞的工具 （3）Metasploit：用于开发和执行漏洞利用代码的框架
密码破解工具	（1）John the Ripper：快速密码破解工具，支持多种加密方式 （2）Hashcat：快速密码恢复工具 （3）Hydra: 强大的登录凭证破解工具，支持多种协议

续表

工具分类	介　　绍
无线安全测试工具	（1）Aircrack-ng：用于破解 IEEE 802.11 WEP 和 WPA-PSK 密钥的工具 （2）Wireshark：网络协议分析工具，可用于网络通信分析和密码数据包捕获
社会工程相关工具	（1）Social-Engineer Toolkit（SET）：专门设计用于模拟社会工程攻击的框架 （2）PhishTank：用于检测网络钓鱼尝试的数据库

1）Nmap

Nmap（网络映射器）是一款用于网络发现和安全审计的开源网络安全工具，常用于主机发现、端口扫描、服务和操作系统的鉴别、漏洞扫描等，Nmap 主界面如图 1-2 所示。

```
└─$ nmap
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

图 1-2　Nmap 主界面

Nmap 通常用在信息收集阶段，用于收集目标主机的基本状态信息。扫描结果可作为漏洞扫描、漏洞利用和权限提升阶段的输入。例如，业界流行的漏洞扫描工具 Nessus 与漏洞利用工具 Metasploit 都支持导入 Nmap 的 XML 格式结果，而 Metasploit 框架也集成了 Nmap 工具（支持 Metasploit 直接扫描）。Nmap 不仅可用于扫描单个主机，也适用于扫描大规模的计算机网络（如扫描互联网）。

Nmap 有以下六大核心功能。

（1）主机发现：用于发现目标主机是否处于活动状态。Nmap 提供了多种用于发现主机的检测机制。

（2）端口扫描：用于扫描主机上的端口状态。Nmap 能够识别端口的多种状态，如开放（Open）、关闭（Closed）、过滤（Filtered）、未过滤（Unfiltered）、开放或过滤（Open/Filtered）、关闭或过滤（Closed/Filtered）等。

（3）版本侦测：用于识别端口上运行的应用程序与程序版本。Nmap 目前可以识别数千种应用的签名（Signatures），检测数百种应用协议。

（4）操作系统侦测：用于识别目标主机的操作系统类型、版本编号及设备类型。Nmap 目前提供 2000 多种操作系统或设备的指纹数据，可识别通用 PC 系统、路由器、交换机等设备类型。

（5）防火墙 /IDS 规避：Nmap 提供多种机制来规避防火墙、IDS（入侵检测系统）的屏蔽和检查，便于秘密地探查目标主机的状况。基本的规避方式包括：数据包分片、IP 诱骗、IP 伪装、MAC 地址伪装。

（6）NSE 脚本引擎：NSE 是 Nmap 最强大、最灵活的特性之一，可用于增强主机发现、端口扫描、版本侦测和操作系统侦测等功能，还可以用来扩展高级功能如 Web 扫描、漏洞发现和漏洞利用等。Nmap 使用 Lua 语言作为 NSE 脚本语言，Nmap 脚本库已经支持数百种脚本。

Nmap 典型用法如下：

```
nmap    [ < 扫描类型 > ...]    [ < 选项 > ]    [< 扫描目标说明 >]
```

2）OpenVAS 工具

OpenVAS（Open Vulnerability Assessment System）是一款开源的漏洞扫描工具，是 Nessus 项目的分支，用于检测目标网络或主机的安全性。它基于 B/S（Browser/Server，浏览器 / 服务器）架构进行工作，执行扫描并提供扫描结果。OpenVAS 主界面如图 1-3 所示。

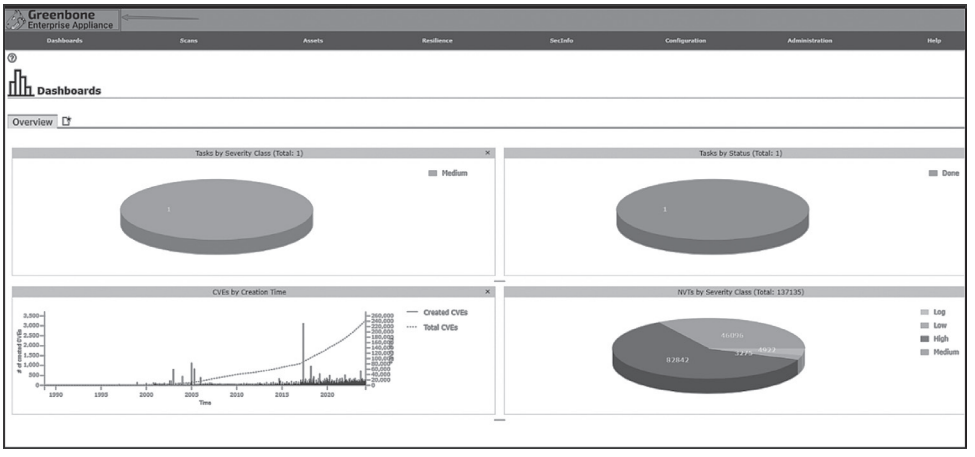

图 1-3　OpenVAS 主界面

OpenVAS 有以下七大核心功能。

（1）全面的漏洞检测：OpenVAS 能够检测多种不同类型的漏洞，包括操作系统漏洞、网络服务漏洞、应用程序漏洞等。它提供了一种综合方式来评估整个网络的安全性。

（2）广泛的漏洞数据库：OpenVAS 使用一个广泛的漏洞数据库，可以检测和识别已知的漏洞，包括常见漏洞及最新的安全威胁。

（3）自定义扫描配置：用户可以自定义扫描配置，以满足其特定需求。这包括配置扫描目标、扫描频率、报告格式等。

（4）报告和结果输出：OpenVAS 会生成详细的扫描报告，其中包含与发现的漏洞、建议的修复措施和风险级别有关的信息。这有助于组织更好地了解其系统的安全状况。

（5）多种操作系统支持：OpenVAS 可以运行在多种不同的操作系统上，包括 Linux、Windows、FreeBSD 等。

（6）可扩展性：OpenVAS 具有可扩展性，支持插件和脚本，允许用户添加自定义检测和报告功能。

（7）Web 用户界面：OpenVAS 附带一个易于使用的 Web 用户界面，使用户能够轻松配置扫描任务、查看报告和管理扫描结果。

3）SQLmap

SQLmap 是一款开源的自动化 SQL 注入和数据库获取工具，可以自动检测和利用 SQL 注入漏洞以及接入该数据库的服务器，SQLmap 主界面如图 1-4 所示。

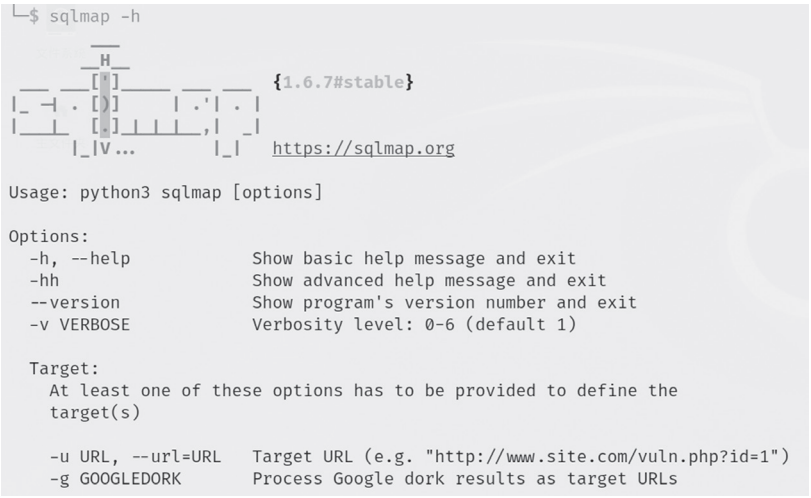

图 1-4　SQLmap 主界面

SQLmap 有以下三大核心功能。

（1）支持多种 SQL 注入技术：Boolean-based Blind、Time-based Blind、Error-based、UNION Query、Stacked Queries 和 Out-of-Band。

（2）支持常见的数据库：MySQL、Oracle、PostgreSQL、Microsoft SQL Server、Microsoft Access、IBM DB2、SQLite、Firebird、Sybase 和 SAP MaxDB。

（3）枚举数据：users、password hashes、privileges、roles、databases、tables 和 columns。

SQLmap 典型用法如下：

```
sqlmap –u < 目标 URL>
```

4）Metasploit

Metasploit 是一个漏洞攻击框架，作为全球最受欢迎的工具，不仅方便使用、功能强大，而且更重要的是它具有灵活的框架，允许用户开发与定制自己的漏洞利用脚本，从而进行个性化测试。Metasploit 主界面如图 1-5 所示。

Metasploit 的主要优势是允许任何攻击代码和任何有效负载进行随意组合，从而实现模块化。用户可以通过不同的搭配在有限的漏洞下导入不同的负载。Metasploit 框架可以通过添加模块实现扩展，允许用户、攻击代码开发者和有效负载的开发者专注于开发所需的功能，而无须处理其他问题。选择攻击代码和有效负载需要目标系统的部分信息，如其操作系统的版本和安装的网络服务。这些信息可被类似于 Nmap 的端口扫描和操作系统分析工具收集到。类似于 Nexpose 或 Nessus 的弱点扫描工具可以探测到目标系统的弱点，Metasploit 可以导入弱点扫描数据，并通过对比已发现的弱点和拥有的攻击代码模块进行准确的攻击。Metasploit 让渗透攻击过程变得异常简单和高效。