Metasploit是一个开源的渗透测试框架软件，也是一个逐步发展成熟的漏洞研究与渗透代码开发平台，此外也将成为支持整个渗透测试过程的安全技术集成开发与应用环境。

## 一．渗透测试框架软件

Metasploit项目由著名黑客HD Moore于2003年开始开发，最早作为一个渗透攻击代码的集成软件包而发布。渗透攻击也是目前Metasploit最强大和最具吸引力的核心功能，Metasploit框架中集成了数百个针对主流操作系统平台上，不同网络服务与应用软件安全漏洞的渗透攻击模块，可以由用户在渗透攻击场景中根据漏洞扫描结果进行选择，并能够自由装配该平台上适用的具有指定功能的攻击载荷，然后通过自动化编码机制绕过攻击限制与检测措施，对目标系统实施远程攻击，获取系统的访问控制权。

Metasploit的出现使得一些渗透测试的初学者也能够像在黑客电影中演的那样“优雅潇洒”地进行渗透攻击，告别了之前令人崩溃与望而却步的繁杂过程：

搜索公开渗透代码→编译→测试→修改代码→实施→失败→不断调试直至成功

正因为如此，Metasploit在发布之后很快得到了安全社区的青睐，成为黑客们与安全职业人员必备的渗透测试工具之一。

除了渗透攻击之外，Metasploit在发展过程中逐渐增加对渗透测试全过程的支持，包括情报搜集、威胁建模、漏洞分析、后渗透攻击与报告生成。

1.情报搜集阶段

Metasploit一方面通过内建的一系列扫描探测与查点辅助模块来获取远程服务信息，另一方面通过插件机制集成调用Nmap、Nessus、OpenVAS等业界著名的开源网络扫描工具，从而具备全面的信息搜集能力，为渗透攻击实施提供必不可少的精确情报。

2.威胁建模阶段

在搜集信息之后，Metasploit支持一系列数据库命令操作直接将这些信息汇总至PostgreSQL、MySQL或SQLite数据库中，并为用户提供易用的数据库查询命令，可以帮助渗透测试者对目标系统搜集到的情报进行威胁建模，从中找出最可行的攻击路径。

3.漏洞分析阶段

除了信息搜集环节能够直接扫描出一些已公布的安全漏洞之外，Metasploit中还提供了大量的协议Fuzz测试器与Web应用漏洞探测分析模块，支持具有一定水平能力的渗透测试者在实际过程中尝试挖掘出“零日”漏洞，并对漏洞机理与利用方法进行深入分析，而这将为渗透攻击目标带来更大的杀伤力，并提升渗透测试流程的技术含金量。

4.后渗透攻击阶段

在成功实施渗透攻击并获得目标系统的远程控制权之后，Metasploit框架中另一个极具威名的工具Meterpreter在后渗透攻击阶段提供了强大功能。

Meterpreter可以看做一个支持多操作系统平台，可以仅仅驻留于内存中并具备免杀能力的高级后门工具，Meterpreter中实现了特权提升、信息攫取、系统监控、跳板攻击与内网拓展等多样化的功能特性，此外还支持一种灵活可扩展的方式来加载额外功能的后渗透攻击模块，足以支持渗透测试者在目标网络中取得立足点之后进行进一步的拓展攻击，并取得具有业务影响力的渗透效果。

从技术角度来说，Meterpreter让它的“前辈们”（如国外的BO、BO2K，以及国内的冰河、灰鸽子等）黯然失色。

5.报告生成阶段

Metasploit框架获得的渗透测试结果可以输入至内置数据库中，因此这些结果可以通过数据库查询来获取，并辅助渗透测试报告的写作。

而商业版本的Metasploit Pro具备了更加强大的报告自动生成功能，可以输出HTML、XML、Word和PDF格式的报告，并支持定制渗透测试报告模板，以及支持遵循PCI DSS（银行支付行业数据安全标准）与FIMSA（美国联邦信息安全管理法案）等标准的合规性报告输出。

正是由于Metasploit最新版本具有支持渗透测试过程各个环节的如此众多且强大的功能特性，Metasploit已经成为安全业界最受关注与喜爱的渗透测试流程支持软件。

Metasploit软件的用户群体也首先面向职业的渗透测试工程师，以及非职业地从事一些渗透测试学习与实践的安全技术爱好者。Metasploit或许是绝大多数渗透测试者最明智的渗透测试工具首选。

真正处于防御一线的网络与系统管理员们也应该熟悉和深入掌握Metasploit，能够自主地对所管理的信息网络进行例行性的白盒式渗透测试，这将有效发现其中的安全薄弱点，在由于真正的入侵发生导致自己挨训甚至丢掉饭碗之前，能够做出有效的补救与防护措施。此外，Metasploit还可以被软件、设备和安全产品测试人员们所使用，特别是在他们工作范围内的某款软件或设备被爆出公开利用的零日安全漏洞时，可以利用Metasploit来重现渗透攻击过程，定位安全漏洞并分析机理，从而修补软件与设备，而诸如IDS、IPS、杀毒软件等安全产品的测试人员，也可以使用Metasploit来检验产品的检测性能，以及针对Metasploit强大免杀与逃逸技术的对抗能力。

## 二．漏洞研究与渗透代码开发平台

当初，HD Moore的理想目标是，让Metasploit成为一个开放的漏洞研究与渗透代码开发的社区公共平台，而这一理想在Metasploit的发展过程中正在得以实现。

当我们在Exploit-db、SecurityFocus等公共渗透代码发布平台上不断发现大量的以Metasploit渗透攻击模块的格式进行编写，能够直接集成到Metasploit框架中进行灵活应用的代码发布时，我们知道已经进入了“Metasploit时代”了！

在“Metasploit时代”之前，黑客社区中的漏洞研究与渗透代码开发是一种“无序化”的状态，大家使用各自掌握的辅助工具和经验挖掘软件安全漏洞，并使用他们自己喜欢的编程语言来开发概念验证性渗透代码（POC），组装上个人珍藏的Shellcode。通常只针对有限的目标版本环境做过初步测试之后，就根据他们自己的“黑客哲学”在直接公开披露、负责任地通告厂商，或进入地下经济链等多种披露策略中做出选择，让他们所发现的安全漏洞和编写的渗透代码进入到安全社区。

采用这种漏洞研究与渗透开发方式所产生的渗透代码往往“鱼龙混杂、混沌不堪”，PacketStorm就是汇集了大量采用此种方式进行安全漏洞完全公开披露的一个代表性网站，每个月几乎都有数百个来自安全社区的漏洞披露与渗透代码发布。对于具有超级信息搜索能力、多种编程语言理解能力、较高渗透技术水平的高级渗透测试师而言，这种汇集大量漏洞与渗透代码的公共信息仓库无疑是一个宝贵的财富，他们有能力在渗透测试过程中快速找到可利用的公开漏洞信息与POC代码，并能够快速通过编译、测试和修改使用到他们自己的渗透过程中。

然而技术能力还不够到位的数量占绝大多数的技术爱好者与初学者，则对这些资源既爱又恨，一方面对找到针对新公开漏洞的渗透代码而欣喜不已，另一方面又没有能力发挥出它的实际效用，这种感受相信绝大多数体验过这一过程的读者们都深有感悟。而HD Moore当初创建Metasploit的想法相信也和他在渗透测试服务中一直遭遇上述境遇是密切相关的。

在“Metasploit时代”，黑客们就可以充分利用Metasploit中针对大量服务协议的Fuzz测试器来辅助他们的漏洞挖掘过程；在发现漏洞之后，他们还可以使用一些调试型的攻击载荷来让漏洞机理分析与利用过程变得更加简单。此外，Metasploit中集成的一系列功能程序可以让他们充分剖析目标程序，并精确定位出利用过程可能依赖的关键指令与地址；在编写渗透代码时，他们也无须从头开始编写代码，从Metasploit开源代码库中找出一个攻击类似目标的模块作为模板，然后将关注点集中在漏洞触发与利用的独特过程，而其他的攻击载荷、协议交互等都可以直接利用框架所提供的支持模块。这样的编写方式不仅省时省力，更为重要的是还具有更为灵活的特性，可以自由的组装任意的攻击载荷；而在测试阶段，黑客们也可以直接使用Metasploit生成测试用例，并可以在多个目标系统测试成功基础上，为渗透代码加上更多的目标系统配置选项，从而提示渗透代码的通用性与鲁棒性。

Metasploit最伟大之处，就是将漏洞研究与渗透代码开发从完全的“手工作坊”形式提升到了初具雏形的“工业化生产方式”，这种贡献足以让它载入安全技术发展的光辉史册。

## 三．安全技术集成开发与应用环境

Metasploit的目标还不仅限于提供一个渗透测试全过程支持框架软件，也不限于作为安全社区的一个开放式漏洞研究与渗透代码开发平台，而是作为一个安全技术的集成开发与应用环境。

你能想象实现这一目标之后Metasploit所具有的能量，以及它在安全社区中的地位吗？那时，Metasploit将成为安全社区中最具影响力的开源框架平台和创新策源地，大量的新技术从这里产出，快速转换成可实际应用与实施的工具，并能够与Metasploit平台上的其他工具相互配合，从而聚集出强大的能量光束，穿透渗透测试过程中的所有目标系统，以及进行安全测试的所有软硬件产品。那时HD Moore和Metasploit核心开发人员则会成为神一级的人物，接受着大家的顶礼膜拜。而这并不是虚无缥缈的幻想，Metasploit正在稳健地迈向这一目标。

首先，Metasploit作为一个开源项目，提供了非常优秀的模块化框架与底层基础库的支持，如果你认同开源理念，完全可以用Metasploit模块的方式来实现新技术与新想法，并贡献到Metasploit的开源代码库中，让安全社区的其他黑客们和渗透测试者都能够分享你的发现与创新。

其次，Metasploit提供了灵活的插件机制和命令行批处理文件机制，已经集成了Nmap、Nessus、OpenVAS等安全社区中重量级的开源或共享安全软件，以及一些极具特色的专项渗透测试工具，如社会工程学工具包SET、自动化攻击软件包Fast Track、无线网络攻击套件Karmetasploit等。而如果期望将自己开发或者社区共享的安全工具加入到Metasploit集成环境中，也可以利用这些机制完成一个“桥”插件，来为Metasploit社区做出贡献。

最后，Metasploit的最新版本实现一个可以远程调用Metasploit内建功能的RPC API接口，利用该接口可以让你更好地使Metasploit和其他一些安全工具进行互操作。

Metasploit社区正在通过一系列努力，朝着构建安全技术集成化开发与应用环境这一宏伟目标前进，是否能达成这一终极目标让我们拭目以待，如果有兴趣和能力，让这一天来的更快些，请贡献出你的智慧和力量吧。