主讲： 屌丝绅士  
时间：11.30晚8.30  
地点：群直播（无YY）  
主题：dmitry 域名/ip 信息收集 不是很难 大牛请绕 谢谢

Deepmagic 信息收集工具

"There be some deep magic going on"

dmitry: 无效的选项 例如 -- '-'

参数: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] 主机

-o 保存输出为host.txt或指定的输出文件的文件

-i 在主机的IP地址进行whois查询

-w 在主机的域名进行WHOIS查询

-n 重新在一个域名上进行信息收集

-s 搜索一个可能存在的子域名

-e 对可能的电子邮件地址进行搜索

-p 在一个主机地址上进行一个tcp端口扫描

\* -f 执行一个TCP端口扫描 在主机上显示哪些端口被过滤

\* -b 从被扫描端口接收的数据中读取

\* -t 0-9 设置TTL秒扫描TCP端口时间( 默认 2 )

\*Requires the -p flagged to be passed

+----------------------------------------------------------------------+

| dnmap 客户端版本 0.6 |

| This program is free software; you can redistribute it and/or modify |

| it under the terms of the GNU General Public License as published by |

| the Free Software Foundation; either version 2 of the License, or |

| (at your option) any later version. |

| |

| 作者: Garcia Sebastian, eldraco@gmail.com |

| www.mateslab.com.ar |

+----------------------------------------------------------------------+

以上是废话！

格式: /usr/bin/dnmap\_client <options> 客户端

参数:

-s, --server-ip dnmap服务器的IP地址。

-p, --server-port 设置dnmap服务器端口。dnmap端口默认为46001

-a, --alias 设置一个别名

-d, --debug 测试

-m, --max-rate 这个参数是使用率最多的. 为了让nmap慢下来 增加了一个最大速率参数

力nmaps命令最多使用率。慢下来，用nmap。添加-最大速率参数。

+----------------------------------------------------------------------+

| dnmap\_server 版本 0.6 |

| 这个程序是免费软件，你可以重新发布它和/或修改 |

|在GNU通用公共许可证的条款公布|

| the Free Software Foundation; either version 2 of the License, or |

| (at your option) any later version. |

| |

| 作者: Garcia Sebastian, eldraco@gmail.com |

| www.mateslab.com.ar |

+----------------------------------------------------------------------+

以上是废话！！！

格式: /usr/bin/dnmap\_server <参数> 服务端

参数:

-f, --nmap-commands Nmap命令文件

-p, --port 监听TCP端口链接

-L, --log-file 默认的日志文件 /var/log/dnmap\_server.conf.

-l, --log-level 默认的日志级别

-v, --verbose\_level Verbose level. Give a number between 1 and 5. 默认s to 1. Level 0 means be quiet.

-t, --client-timeout 我们要等待多少时间在离线标记客户端。我们还记得它的值，万一它回来。.

-s, --sort 排序字段的静态值. 你可以这样选择: Alias, #Commands, UpTime, RunCmdXMin, AvrCmdXMin, Status

-P, --pem-file PEM文件使用TLS连接. 默认情况使用服务器当前目录中的PEM文件。

dnmap\_server 如果你想重新开始 就使用一个 '<nmap-commands-file-name>.dnmaptrace' 文件，使用它必须阅读NMAP命令文件.而不是删除'<nmap-commands-file-name>.dnmaptrace' 文件

格式: ike-scan [options] [hosts...]

目标主机必须在命令行上指定，除非-file选项是给定的，在这种情况下，目标是从指定的文件读取，而不是直接输入

目标主机可以被指定为IP地址或主机名。你也可以指定IP网络/位（例如192.168.1.0／24）指定在给定的所有主机网络（网络和广播地址包含，和IPstart IPend（192.168.1.3-192.168.1.27）在包容范围内指定的所有主机。

这些不同的选项用于指定目标主机上的可用的命令行，并在指定的文件中指定的文件选项。

在下面的选项中的一个字母或字的角度括号如“F”表示一个应该提供的值或字符串。相应的文本应该指示此值或字符串的含义。当提供准确的表示服或字符串，不包括角括号。方括号中的文本。

一个可选的参数

参数:

--help or -h 显示帮助文件

--file=<fn> or -f <fn> 从指定的文件中读取主机名或地址 而不是从命令行。

--sport=<p> or -s <p> 设置一个UDP端口 <p>, 默认=500, 0=随机.

一些IKE实现要求客户端使用UDP源端口500不会跟其他端口。请注意，通常需要超级用户权限使用1024以下的非零源端口。也只有一个系统上的一个进程可能绑定到一个给定的源端口在任何一个时间。使用--nat-t改变默认源端口为4500

--dport=<p> or -d <p> UDP目的端口设置为，默认值为500。

UDP端口500是分配的端口号为ISAKMP，这是用得最多的端口，如果不是所有的ike实现。使用--nat-t改变默认端口到4500

--retry=<n> or -r <n> 将主机的总次数设置为多少 默认=3.

--timeout=<n> or -t <n> 设置每个主机的超时时间 <n> ms, 默认=500.

此超时是用于发送给每个主机的第一个数据包。

subsequent timeouts are multiplied by the backoff factor which is set with --backoff.

--bandwidth=<n> or -B <n> Set desired outbound bandwidth to <n>, 默认=56000

该值是在每第二位默认. 如果你把“K”的价值，然后，单位是千字节每秒；如果你把“M”的价值，单位是兆比特每秒。

“K”和“M”后缀表示十进制，二进制，倍数。所以64K时64000，不是65536。

--interval=<n> or -i <n>设置最小数据包间隔 <n> ms.

分组间隔将不小于这个数字 指定的间隔在默认的毫秒内.如果“U”是附加的价值，那么周期是微秒，如果“S”追加，间隔秒。如果你想使用一个给定的带宽，那么它更容易使用 ndwidth选项。你不能指定两个-间隔和-带宽，因为他们只是不同的方式来改变相同的基本变量。

--backoff=<b> or -b <b> Set timeout backoff factor to <b>, 默认=1.50.

每个主机超时乘以这个因素在每个超时。所以，如果重试次数是3，初始每个主机超时500ms和退避因子是1.5，那么第一个超时会 l 500ms，二750ms，第三1125ms。

--verbose or -v 显示详细的进度消息。

使用不止一次，效果更大：

1 - Show when each pass is completed and when

packets with invalid cookies are received.

2 - Show each packet sent and received and when

hosts are removed from the list.

3 - Display the host, Vendor ID and backoff lists

before scanning starts.

--quiet or -q 不要对返回的数据包进行解码。

这打印更少的协议信息，所以输出线较短。

--multiline or -M 通过拆分多行的有效负载解码。

有了这个选项，每个有效载荷的解码打印在一个单独的行开始与标签。此选项使输出更容易阅读，尤其是当有许多有效载荷。

--lifetime=<s> or -l <s> Set IKE lifetime to <s> seconds, 默认=28800.

RFC 2407 specifies 28800 as the 默认, but some implementations may require different values.

如果指定为一一的十进制整数，如86400，然后将属性将使用一个4字节值。如果你将它指定为十六进制数，如0xff，那么属性将使用适当大小的价值 （这个例子的一个字节）。如果你指定了字符串“没有”，那么没有生命周期的属性将被添加在所有。您可以使用此选项不止一次配合——经选择产品 多变换载荷不同的寿命。每一个-跨选项将使用先前指定的生命值。

--lifesize=<s> or -z <s> Set IKE lifesize to <s> Kilobytes, 默认=0.

If you specify this as a a decimal integer, e.g.

86400, then the attribute will use a 4-byte value.

If you specify it as a hex number, e.g. 0xFF, then

the attribute will use the appropriate size value

(one byte for this example).

You can use this option more than once in conjunction

with the --trans options to produce multiple transform

payloads with different lifesizes. Each --trans option

will use the previously specified lifesize value.

--auth=<n> or -m <n> Set auth. method to <n>, 默认=1 (PSK).

RFC defined values are 1 to 5. See RFC 2409 Appendix A.

Checkpoint hybrid mode is 64221.

GSS (Windows "Kerberos") is 65001.

XAUTH uses 65001 to 65010.

This is not applicable to IKEv2.

--version or -V Display program version and exit.

--vendor=<v> or -e <v> Set vendor id string to hex value <v>.

You can use this option more than once to send

multiple vendor ID payloads.

--trans=<t> or -a <t> Use custom transform <t> instead of 默认 set.

You can use this option more than once to send

an arbitrary number of custom transforms.

There are two ways to specify the transform:

The new way, where you specify the attribute/value

pairs, and the old way where you specify the values

for a fixed list of attributes.

For the new method, the transform <t> is specified as

(attr=value, attr=value, ...)

Where "attr" is the attribute number, and "value" is

the value to assign to that attribute. You can specify

an arbitary number of attribute/value pairs.

See RFC 2409 Appendix A for details of the attributes

and values.

Note that brackets are special to some shells, so you

may need to quote them, e.g.

--trans="(1=1,2=2,3=3,4=4)". For example,

--trans=(1=1,2=2,3=1,4=2) specifies

Enc=3DES-CBC, Hash=SHA1, Auth=shared key, DH Group=2;

and --trans=(1=7,14=128,2=1,3=3,4=5) specifies

Enc=AES/128, Hash=MD5, Auth=RSA sig, DH Group=5.

For the old method, the transform <t> is specified as

enc[/len],hash,auth,group.

Where enc is the encryption algorithm,

len is the key length for variable length ciphers,

hash is the hash algorithm, and group is the DH Group.

For example, --trans=5,2,1,2 specifies

Enc=3DES-CBC, Hash=SHA1, Auth=shared key, DH Group=2;

and --trans=7/256,1,1,5 specifies

Enc=AES-256, Hash=MD5, Auth=shared key, DH Group=5.

This option is not yet supported for IKEv2.

--showbackoff[=<n>] or -o[<n>] Display the backoff fingerprint table.

Display the backoff table to fingerprint the IKE

implementation on the remote hosts.

The optional argument specifies time to wait in seconds

after receiving the last packet, 默认=60.

If you are using the short form of the option (-o)

then the value must immediately follow the option

letter with no spaces, e.g. -o25 not -o 25.

--fuzz=<n> or -u <n> Set pattern matching fuzz to <n> ms, 默认=500.

This sets the maximum acceptable difference between

the observed backoff times and the reference times in

the backoff patterns file. Larger values allow for

higher variance but also increase the risk of

false positive identifications.

Any per-pattern-entry fuzz specifications in the

patterns file will override the value set here.

--patterns=<f> or -p <f> Use IKE backoff patterns file <f>,

默认=/usr/share/ike-scan/ike-backoff-patterns.

This specifies the name of the file containing

IKE backoff patterns. This file is only used when

--showbackoff is specified.

--vidpatterns=<f> or -I <f> Use Vendor ID patterns file <f>,

默认=/usr/share/ike-scan/ike-vendor-ids.

This specifies the name of the file containing

Vendor ID patterns. These patterns are used for

Vendor ID fingerprinting.

--aggressive or -A Use IKE Aggressive Mode (The 默认 is Main Mode)

If you specify --aggressive, then you may also

specify --dhgroup, --id and --idtype. If you use

custom transforms with aggressive mode with the --trans

option, note that all transforms should have the same

DH Group and this should match the group specified

with --dhgroup or the 默认 if --dhgroup is not used.

--id=<id> or -n <id> Use <id> as the identification value.

This option is only applicable to Aggressive Mode.

<id> can be specified as a string, e.g. --id=test or as

a hex value with a leading "0x", e.g. --id=0xdeadbeef.

--idtype=<n> or -y <n> Use identification type <n>. 默认 3 (ID\_USER\_FQDN).

This option is only applicable to Aggressive Mode.

See RFC 2407 4.6.2 for details of Identification types.

--dhgroup=<n> or -g <n> Use Diffie Hellman Group <n>. 默认 2.

This option is only applicable to Aggressive Mode and

IKEv2. For both of these, it is used to determine the

size of the key exchange payload.

If you use Aggressive Mode with custom transforms, then

you will normally need to use the --dhgroup option

unless you are using the 默认 DH group.

Acceptable values are 1,2,5,14,15,16,17,18 (MODP only).

--gssid=<n> or -G <n> Use GSS ID <n> where <n> is a hex string.

This uses transform attribute type 16384 as specified

in draft-ietf-ipsec-isakmp-gss-auth-07.txt, although

Windows-2000 has been observed to use 32001 as well.

For Windows 2000, you'll need to use --auth=65001 to

specify Kerberos (GSS) authentication.

--random or -R Randomise the host list.

此选项randomises在主人的命令主机列表，所以艾克探针发送给主机随机顺序。 它使用Knuth洗牌算法。

--tcp[=<n>] or -T[<n>] 相反，利用UDP传输。

这允许您测试主机的TCP IKE。

你不需要这个选项，因为绝大多数的IPSec系统只支持IKE UDP。

可选值<n>指定协议类型TCP。目前有两种可能的值：

1 = 原艾克TCP所使用的检查点(默认);

2 = 艾克TCP封装用思科。

如果您使用的是期权的缩写形式（T）的值必须紧跟选项字符没有空格，如T2不T 2。 如果您使用此选项，您只能指定一个目标主机。

--tcptimeout=<n> or -O <n> Set TCP connect timeout to <n> seconds (默认=10).

这是只适用于TCP传输模式。

--pskcrack[=<f>] or -P[<f>] Crack aggressive mode pre-shared keys.

这个选项输出攻击模式预共享密钥（PSK）用“PSK破解”程序，提供艾克开裂离线参数扫描。

您可以选择指定一个文件名，<f>，写的PSK参数。如果你不指定一个文件名然后PSK参数写入标准输出。如果你使用的是短形式的 选项（P）的值必须紧跟选项字符没有空格，例如Pfile不是P文件。如果您使用此选项，您只能指定一个目标主机。

此选项仅适用于艾克攻击模式。

--nodns or -N Do not use DNS to resolve names.

如果您使用此选项，则所有主机必须被指定为IP地址。

--noncelen=<n> or -c <n> Set the nonce length to <n> bytes. 默认=20

这个选项控制长度的临时载荷发送一个模式或IKEv2的要求。通常不需要使用这个选项，除非你想减少现时规模加快预共享密钥破解，或者如果你想看到一个特定的服务器处理不同长度的随机数 有效载荷。RFC 2409指出，现时有效载荷的长度必须是8和256字节之间，但艾克扫描不执行。指定一个大的临时的长度会增加大小的包在艾克扫描发。一个非常大的临时的长度可能会导致分裂，或超过最大IP数据包大小。此选项仅适用于艾克攻击模式。

--headerlen=<n> or -L <n> Set the length in the ISAKMP header to <n> bytes.

您可以使用此选项来手动指定的值可用于ISAKMP报头长度。通过默认，艾克扫描将填写正确的价值。使用此选项手动指定一个不正确的长度。

<n> 可以被指定为“+ N”，它将长度设置为N个字节，而不是它应该是“N”，它将它设置为n个字节，或“N”，它将它设置为完全字节。

改变页眉长度不正确的值有时会破坏VPN服务器。

--mbz=<n> or -Z <n> Use the value <n> for reserved (MBZ) fields, 默认=0.

指定此选项使传出的数据包不符合RFC标准，只应使用如果你想看看一个VPN服务器将响应无效的数据包。价值<n>应该范围在0-255。

--headerver=<n> or -E <n> 指定ISAKMP报头版。

是的默认0x10（16）对应v1.0。指定一个非默认值将发送出去的数据包不符合RFC标准，只应如果你想看到VPN服务器如何使用奇怪的反应 E版本。该值应该是范围在0-255。

--certreq=<c> or -C <c> 添加certificaterequest载荷 <c>.

<c> 应指定为十六进制值。

第一个字节的十六进制值将被解释为证书类型；剩余的字节为证书权威在RFC 2408中描述3.10。

证书类型列在RFC 2408秒3.9。RFC 2048州“证书请求负载必须接受在任何时候在交流”

--doi=<d> or -D <d> Set the SA DOI to <d>, 默认 1 (IPsec).

你将不想改变这个除非你想看到VPN服务器如何响应标准。

--situation=<s> or -S <s> Set the SA Situation to <d>, 默认 1.

形势的意义取决于我，是在适当的DOI文档详细。对IPsec DOI，1默认情况代表sit\_identity\_only。你将不想改变这个除非你想看到VPN服务器如何响应一个非标准的情况。

--protocol=<p> or -j <p> 将建议协议标识设置为<p>, 默认 1.

提议的协议识别的意义取决于语言，并在适当的DOI文档详细。对IPsec DOI的1默认建议协议ID代表proto\_isakmp。

你将不想改变这个除非你想看到VPN服务器如何非标准协议的响应

--transid=<t> or -k <t> Set the Transform ID to <t>, 默认 1.

该变换身份取决于我的意义，并在适当的DOI文档详细。对IPsec DOI的默认变换身份1代表key\_ike。

你将不想改变这个除非你想看到VPN服务器如何响应规范变换的ID。

--spisize=<n> Set the proposal SPI size to <n>. 默认=0

如果是非零，那么随机SPI指定的大小将被添加到建议的有效载荷。

零意味着没有SPI的默认。

--hdrflags=<n> Set the ISAKMP header flags to <n>. 默认=0

旗帜在RFC 2408中3.1节作详细介绍

--hdrmsgid=<n> Set the ISAKMP header message ID to <n>. 默认=0

这应该是零，艾克期。

--cookie=<n> Set the ISAKMP initiator cookie to <n>

应在十六进制中指定该值的值。

通过默认，饼干是自动生成的，具有独特的价值。如果指定此选项，那么你只能指定一个目标，因为艾克扫描需要唯一的cookie的值匹配 响应数据包。

--exchange=<n> Set the exchange type to <n>

这个选项允许你改变交换式在ISAKMP头一个任意值。

注意，艾克扫描只支持主要的攻击方式（值2和4分别）。指定其它值将在ISAKMP头改变交换类型的值，但不调整其他 R的有效载荷。

交换类型定义在RFC 2408秒3.1。

--nextpayload=<n>在ISAKMP头设置下的载荷 <n>

通常情况下，下一个有效负载将被自动设置为正确的值。

--randomseed=<n> Use <n>种子伪随机数发生器。

此选项指定数目的PRNG种子，可如果你想确保分组数据是完全重复时，它包括随机数据等关键性的有效载荷 GE或杜撰。

通过默认PRNG种子，是不可预知的价值。

--timestamp 对接收到的数据包的时间戳显示。此选项将使时间戳是每个接收到的分组显示。

--sourceip=<s> 设置用于发送数据包的源IP地址<s>.

此选项将使即将离任的IKE包有指定的源IP地址。地址可以是一个点的四分格式的IP地址，或字符串“随机”，将使用不同的 随机的源地址为每个数据包被发送。如果使用此选项，没有数据包将收到此选项需要原始套接字支持，你将需要管理员权限才能使用该选项 ，即使您指定了一个高源端口。此选项不在所有操作系统上工作。

--shownum Display the host number for received packets.

显示在IP地址之前响应主机的序号主机号。它可以是有用的，当发送多个数据包到相同的目标IP，看看是否有任何探针被忽略。

--nat-t Use RFC 3947 NAT-Traversal encapsulation.

这个选项会增加非ESP标记从接收到的数据包传出的数据包，带它开始，在RFC 3947中描述。它也改变了默认源端口为4500，默认目的 n端口4500，这是遍历IKE端口。这些端口号可以改变-运动和

--dport options, 提供他们使用后

--nat-t option.

--rcookie=<n> Set the ISAKMP responder cookie to <n>.

这将响应器设置为指定的十六进制值。通过默认，响应Cookie设置为零。

--ikev2 or -2 Use IKE version 2

这会导致输出的数据包使用RFC 4306中定义的格式而不是默认IKEv1协议格式。任何数据包返回自动解码为艾克或IKEv2取决于其有效载荷的我 rrespective这个选项。

——IKEv2选项是目前实验。它没有被广泛的测试，它只支持发送默认建议。

Report bugs or send suggestions to ike-scan@nta-monitor.com

See the ike-scan homepage at http://www.nta-monitor.com/tools/ike-scan/

netdiscover: 无效的选项 -- '-'

Netdiscover 0.3-pre-beta7 [Active/passive arp reconnaissance tool]

Written by: Jaime Penalba <jpenalbae@gmail.com>

以上是作者的联系方式

格式: netdiscover [-i 方法] [-r 范围 | -l ip地址文件 | -p] [-m mac地址文件] [-s 时间] [-n node] [-c count] [-f] [-d] [-S] [-P] [-c]

-i device: 查看你的网络设备

-r range: 扫描一个给定的范围，而不是自动扫描例如192.168.6.0/24,/16,/8

-l file: 扫描文件中的地址

-p passive mode: 不要发送任何东西，只有嗅探

-m file: 扫描列表中已知的MAC地址和主机名

-F filter:自定义PCAP筛选器表达式（默认方式为: "arp")

-s time: 每个ARP请求之间时间间隔（毫秒）

-n node: 用最后一个IP字节扫描 (默认从 2 to 253)

-c count: 多次发送ARP请求(for nets with packet loss)

-f 使用 快速模式扫描, 省时间扫描, recommended for auto

-d 忽视主机配置文件 自动扫描和快速模式

-S 使每个请求的时间限制(hardcore mode)

-P 显示输出错误的地方

-N 禁止输出头部信息 使用-P 才会被启用

-L 在解析输出模式 (-P), 主动扫描完成后继续监听

-r, -l or -p 不启用, netdiscover 将扫描常见的局域网地址。

--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

以上输出的是版本号作者以及作者的联系方式

p0f: 无效的选项 -- '-'

格式: p0f [ ...options... ] [ 'filter rule' ]

网络接口选项:

-i iface - 在指定的网络接口上侦听

-r file - 从一个给定的文件中读取数据的离线PCA

-p - 把监听接口设置成混杂模式

-L -列出所有可用的接口

操作模式和输出设置:

-f file - 从“文件”中读取指纹数据库(/etc/p0f/p0f.fp)

-o file - 将信息写入指定的日志文件

-s name - 在一个UNIX套接字上 用API查询应答

-u user - 切换到指定的非特权帐户和chroot

-d -插入背景(requires -o or -s) ？？？？

性能相关的选项:

-S limit - 并行连接的连接的限制数目（20）

-t c,h - 设置连接/主机缓存的大小（30M、120M）

-m c,h - 活动连接/主机的数量 (1000,10000)

Problems? You can reach the author at <lcamtuf@coredump.cx>.

格式: recon-ng [-h] [-v] [-w workspace] [-r 文件名] [--no-check]

[--no-analytics]

recon-ng - Tim Tomes (@LaNMaSteR53) tjt1980[at]gmail.com

以上是作者的联系方式

可选参数:

-h, --help 显示此帮助消息并退出

-v, --version 显示程序的版本号和退出

-w workspace 加载/创建一个工作区

-r filename 从资源文件中加载命令

--no-check 禁用版本检查

--no-analytics 不生成报告