Amap

> 识别运行端口上的应用程序

这是Amap的公开发布。Amap是圣诞节的下一代扫描工具。它试图识别应用程序，即使它们运行在与正常端口不同的端口上。

它还识别非ascii应用程序。这是通过发送触发数据包，并在响应字符串列表中查找响应来实现的。

如果没有包含触发器和响应的填充数据库，该工具就毫无价值，所以我请求您帮助我们填充数据库。怎么做？

每当一个客户端应用程序连接到一个服务器时，某种握手就被交换了(至少通常是这样。例如，Syslogd不会说什么，snmpd也不会没有正确的社区字符串)。无论如何，amap会将第一个返回的数据包与签名响应列表进行比较。

实际上非常简单。事实上，至少对大多数协议来说，这真的很简单。

现在，通过amap，您可以识别在端口3442上运行的SSL服务器，以及在端口23上运行的Oracle侦听器。

对于未知协议，您可以使用amapcrap(向audp、tcp或ssl端口发送随机垃圾)来非法响应，然后将其放入appdefs.trig和appdefs.resp文件中。

——*by van Hauser and DJ RevMoon / THC amap-dev@thc.org*

一，帮助手册

```
语法:AMAP[-A |-B |-P |-W][-1BushHudQv][[-m]-o &lt; file &gt;][-D &lt; file
&gt;][-T/-T秒] [-c cons] [-C重试] [-p协议][-I &lt; file &gt;][目标端口[端口]...]

模式:
-A  映射应用程序:发送触发器和分析响应(默认)
-B  只需抓住横幅，不要发送触发器
-P  没有横幅或应用程序的东西-是一个(完全连接)端口扫描仪

选择:
-1  仅向端口发送触发器，直到第一次识别。演讲！

-6  使用IPv6而不是IPv4

-b  打印回应的ascii横幅

-i  文件 要从中读取端口的文件Nmap机器可读输出文件

-u  命令行上指定的端口是UDP(默认为TCP)
```

```
-R  不要识别RPC服务

-H  不要发送标记为潜在有害的应用程序触发器

-U  不要转储未识别的响应(最好是脚本)

-d  转储所有响应

-v  详细模式，使用两次(或更多次！)进行调试(不推荐:-)

-q  不要报告关闭的端口，也不要将其打印为未识别的端口

-o  文件  [-m]将输出写入文件文件，-m创建机器可读输出

-c  CONS要建立的并行连接数(默认32，最大256)

-C  重试次数 连接超时时重新连接的次数(参见-T)(默认为3)

-T  秒 以秒为单位的连接超时(默认为5

-t  秒 以秒为单位的响应等待超时(默认为5)

-p  原型 仅发送此协议的触发器(例如ftp)
```

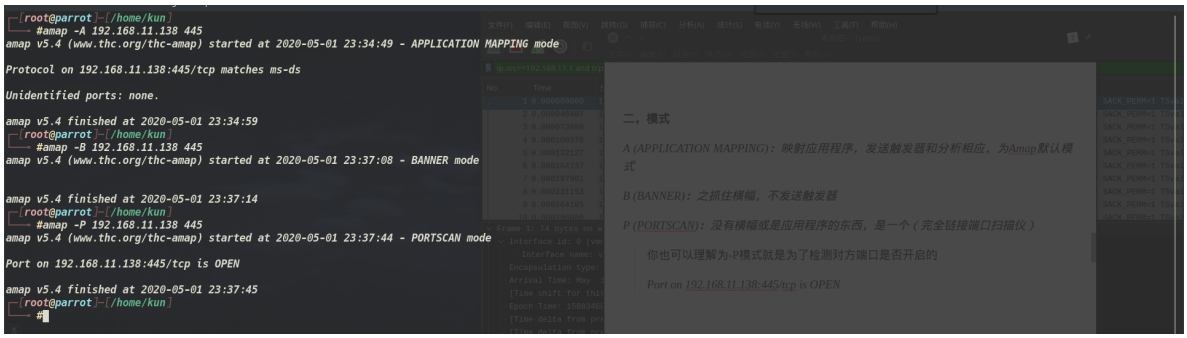
目标端口要扫描的目标地址和端口(除-i之外)，用法提示:建议使用选项“-bqv”，快速/紧急检查时添加“-1”。
amap是识别目标端口上的应用协议的工具。注意:这个版本不是用SSL支持编译的！
用法提示:建议使用选项“-bqv”，快速/紧急检查时添加“-1”。

```
amap v5.4 (c) 2011 by van Hauser <vh@thc.org> www.thc.org/thc-amap
```

```
Syntax: amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>] [-D <file>] [-t/-T
sec] [-c cons] [-C retries] [-p proto] [-i <file>] [target port [port] ...]
Modes:
  -A         Map applications: send triggers and analyse responses (default)
  -B         Just grab banners, do not send triggers
  -P         No banner or application stuff - be a (full connect) port scanner
Options:
  -1         Only send triggers to a port until 1st identification. Speeeeed!
  -6         Use IPv6 instead of IPv4
  -b         Print ascii banner of responses
  -i FILE    Nmap machine readable outputfile to read ports from
  -u         Ports specified on commandline are UDP (default is TCP)
  -R         Do NOT identify RPC service
  -H         Do NOT send application triggers marked as potentially harmful
  -U         Do NOT dump unrecognised responses (better for scripting)
  -d         Dump all responses
  -v         Verbose mode, use twice (or more!) for debug (not recommended :-)
  -q         Do not report closed ports, and do not print them as unidentified
  -o FILE [-m] Write output to file FILE, -m creates machine readable output
  -c CONS    Amount of parallel connections to make (default 32, max 256)
  -C RETRIES Number of reconnects on connect timeouts (see -T) (default 3)
  -T SEC     Connect timeout on connection attempts in seconds (default 5)
  -t SEC     Response wait timeout in seconds (default 5)
  -p PROTO   Only send triggers for this protocol (e.g. ftp)
```

```
  TARGET PORT   The target address and port(s) to scan (additional to -i)
amap is a tool to identify application protocols on target ports.
Note: this version was NOT compiled with SSL support!
Usage hint: Options "-bqv" are recommended, add "-1" for fast/rush checks.
```

二，模式



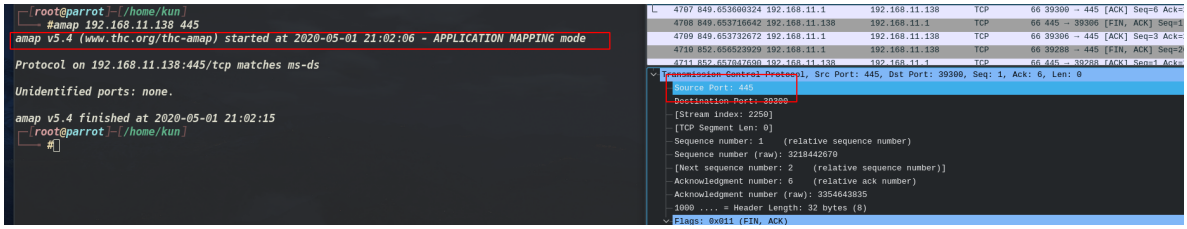
A (APPLICATION MAPPING)：映射应用程序，发送触发器和分析相应，为Amap默认模式

B (BANNER)：之抓住横幅，不发送触发器

P (PORTSCAN)：没有横幅或是应用程序的东西，是一个（完全链接端口扫描仪）

> 你也可以理解为-P模式就是为了检测对方端口是否开启的
>
> *Port on 192.168.11.138:445/tcp is OPEN*

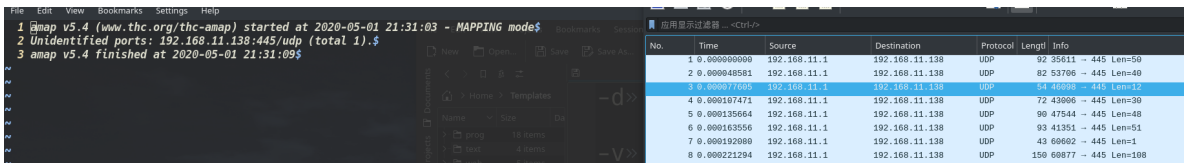
三，命令实例



amap 192.168.11.138 445

查找对方开放的445端口对应的相关协议及应用。

> 如果你想要查看一些非常详细的端口信息，可以通过http://zsdk.org.cn/zsdk/445.html 来查看445端口的详细信息及相关方面的漏洞

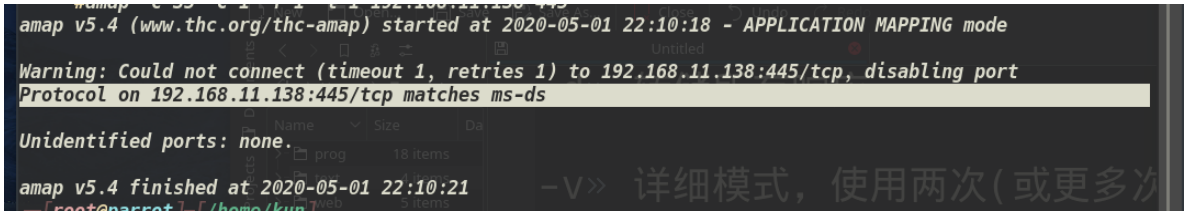


amap -u -o 192 192.168.11.138 445

使用udp模式对目标445端口进行检索，并将结果以人类可读的形式导出

```
# amap v5.4 (www.thc.org/thc-amap) started at 2020-05-01 21:34:39 - MAPPING mode$
# IP_ADDRESS:PORT:PROTOCOL:PORT_STATUS:SSL:IDENTIFICATION:PRINTABLE_BANNER:FULL_BANNER$
192.168.11.138:445:tcp:open::ms-ds:USMBrS2E G e1ayz:0x00000055ff534d4272000000009853c80000000000000
000000000000000fffe00000000110500033200010004110000000001000000000fdf30180d0170545bd1fd60120fe0010
00081f128912a59f47998420653161797a$
# Unidentified ports: none.$
# amap v5.4 finished at 2020-05-01 21:34:48$
```

> amap -m -o 192 192.168.11.138 445
>
> 将检索之后的结果以机器可读的形式导出



amap -c 35 -C 1 -T 1 -t 192.168.11.138

设置CONS（面向连接服务）建立并发数为35,anap默认为“35 ~ 256” ，重试连接数目为“1”[^默认为3,单位为秒]，连接超时时间为”1“，等待超时时间为”1“[^-T与-t默认为3 。单位为秒]

> 面相连接服务，在通信双方进行通信时，要事先建立一条通信线路，其过程主要有建立链接，使用链接和释放链接三个过程。就比如TCP连接，也属于面向连接的一种。
>
> 而面向连接服务的特点就是，你如果想连接我，那你必须给我建立一条连接线路。然后当你用完了这个管道的时候，那你需要关闭这个管道
>
> 这就跟你买房一样，你可以自己慢慢联想一下，首付就是建立链接，还款就是使用链接，还款完后就是关闭链接。

amnp -v 192.168.11.138 445

详细模式，第一次可能会比较慢，当你多尝试几次的话，那就可以享受到用户体验了。

> 远程过程调用协议（RPC，Remote Procedure Call Protocol），他是一种通过网路哦从远程计算机程序上请求服务，而不需要了解网络底层技术的协议。
>
> 该协议主要用于允许一台计算机的程序访问另一台计算机的子程序，而开发人员无需为此特地搞一个交互式作用的编程。

amap -R 192.168.11.138 445

不识别PRC服务。

> amap -q 192.168.11.138 445
>
> 不报告关闭的端口，也不要将其打印为未识别的端口

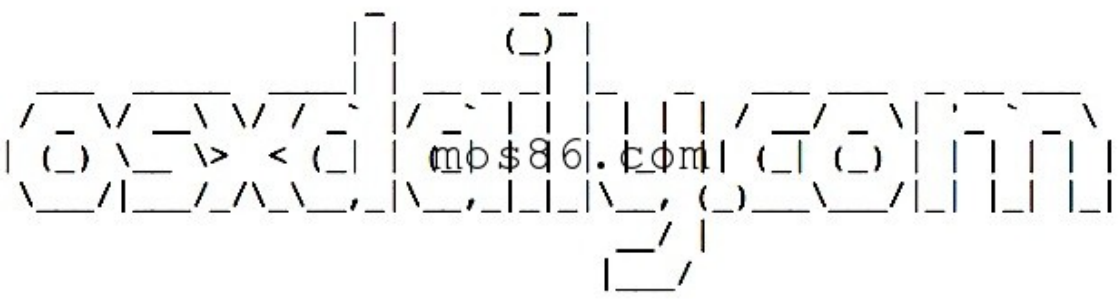
ASCII表

(American Standard Code for Information Interchange 美国标准信息交换代码)

高四位 / 低四位		ASCII控制字符 0000 0						ASCII控制字符 0001 1						ASCII打印字符 0010 2		ASCII打印字符 0011 3		ASCII打印字符 0100 4		ASCII打印字符 0101 5		ASCII打印字符 0110 6		ASCII打印字符 0111 7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。 2013/08/08

> ASCII(American Standard Code for Information Interchange，美国信息交换标准代码)是基于拉丁字母的一套电脑编码系统，主要用于显示现代英语和西欧语言，他是通用的信息交换标准，并同等与国际标准ISO/IEC 646
>
> 而ACSII横幅，就类似与下图：



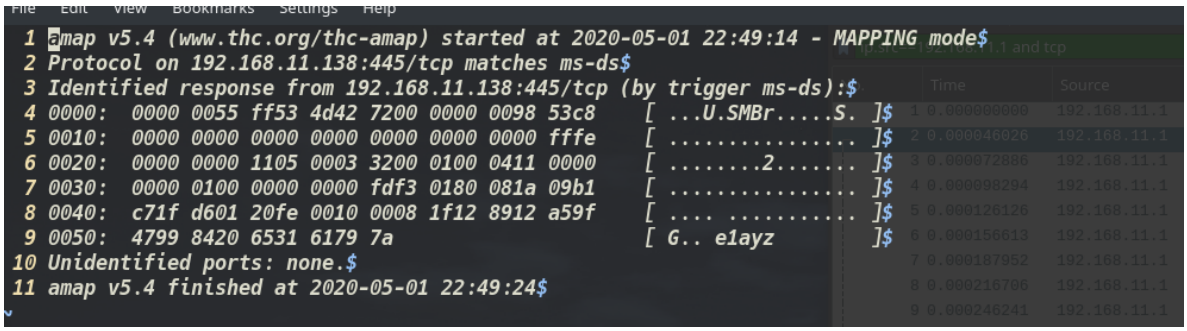
> 当然你可以使用banner 生成一个类似的

amap -b 192.168.11.138 445

打印回应的ascii横幅

> 转储(Dump)

> 转储就是将一个动态易丢失的数据保存为静态不易改变的数据。



amap -d -o zs 192.168.11.138 445

将所有响应数据转储到zs文本文件之中

> amap -U 192.168.11.138 445
>
> 转储为识别的响应（最好配合-o）一起用

> 触发器（Trigger）是一个特殊的存储过程，他的执行不是由程序掉通用，也不是手工启动。而是当某一个事件触发的。而简单的可以理解为，与表时间和相关特殊的存储过程。

> amap -1 192.168.11.138
>
> 仅向目标端口发送触发器，直到第一次识别。
>
> amap -p ftp 192.168.11.138 445
>
> 发生一个ftp类型的触发器
>
> amap -H 192.168.11.138 445
>
> 不要发送标记为潜在有害的程序触发器