主讲： 屌丝绅士  
时间：12.14 晚 8.30  
地点：群直播（无YY）  
主题：smtp分析 不是很难 大牛请绕 谢谢

running under Perl version 5.24.1.

格式: smtp-user-enum [-OPTIONS [-MORE\_OPTIONS]] [--] [PROGRAM\_ARG1 ...]

以下的单字符选项被接受：

With arguments: -m -u -U -s -S -r -t -M -f -D -p

Boolean (without arguments): -d -v -h

选项可以合并在一起。 -- stops processing of options.

选项和它们之间的参数之间不需要空格。

[Now continuing due to backward compatibility and excessive paranoia.

See 'perldoc Getopt::Std' about $Getopt::Std::STANDARD\_HELP\_VERSION.]

smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

格式: smtp-user-enum.pl [options] ( -u username | -U file-of-usernames ) ( -t host | -T file-of-targets )

选项:

-m n 最大进程数（默认值：5）

-M mode 使用用户名猜测或者方法，RCPT（默认：VRFY）

-u user 检查远程系统上是否存在EXPN VRFY用户

-f addr 电子邮件地址。只用于“RCPT”模式（默认：[user@example.com）](mailto:user@example.com）)

-D dom 域添加到提供的用户列表，以使电子邮件地址（默认：无）

当你要想有效的电子邮件地址而不是用户使用此选项 e.g. "-D example.com" would guess foo@example.com, bar@example.com, etc. 而不是简单的用户名Foo和Bar。

-U file 文件的用户名检查通过SMTP服务

-t host 服务器主机上运行SMTP服务

-T file 对主机运行SMTP服务文件

-p port TCP端口，SMTP服务运行（默认值：25）

-d 调试输出

-t n 等待最多N秒的答复（默认为：5）

-v 详细输出

-h 这个信息帮助

Also see smtp-user-enum-user-docs.pdf from the smtp-user-enum tar ball.

实例:

$ smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1

$ smtp-user-enum.pl -M EXPN -u admin1 -t 10.0.0.1

$ smtp-user-enum.pl -M RCPT -U users.txt -T mail-server-ips.txt

$ smtp-user-enum.pl -M EXPN -D example.com -U users.txt -t 10.0.0.1