Enumeração SMTP

Outra forma efetiva de obter informações de um alvo é através do uso do SMTP. Este protocolo foi desenhada para enviar mensagens entre servidores que enviam e recebem e-mails. SMTP é um padrão usado pela maioria dos servidores e clientes de e-mail hoje em dia.

Então, como podemos usar este protocolo para obter informações? O processo é simples se você tiver o conhecimento fundamental de alguns comandos e como usá-los.

Usando o VRFY

Uma forma fácil de verificar a existência de contas de e-mails em um servidor usando o comando telnet para anexar o alvo e extrair informações. O comando VRFY é usado dentro do protocolo para checar se um ID de usuário específico está presente. Entretanto, o mesmo comando pode ser usado por um atacante para localizar contas válidas para atacar, e se usar um script, pode ser usada para extrair várias contas em pouco tempo, como mostrado abaixo:

```
telnet 10.0.0.1 25 (where 10.0.0.1 is the server IP and 25 is the port for SMTP)
220 server1 ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 server1 Hello [10.0.0.72], pleased to meet you
VRFY chell
250 Super-User <link@server1>
VRFY glados
550 glados... User unknown
```

O código usa o VRFY para validar contas de usuários chamado de *chell* e *glados*. O servidor responde com informações indicando que o usuário *chell* é válido, já o usuário *glados* tem como

resposta *User unknow*.

Usando o EXPN

O comando é similar ao VRFY, mas ao invés de retornar um usuário, ele retorna todos os usuários de uma lista de distribuição:

```
telnet 10.0.0.1 25 (where 10.0.0.1 is the server IP and 25 is the port for SMTP)
220 server1 ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 server1 Hello [10.0.0.72], pleased to meet you
EXPN link
250 Super-User <link@myhost>
EXPN zelda
550 zelda... User unknown
```

Assim como o VRFY, o EXPN pode ser desativado em alguns casos, mas antes de fazer isto é importante ter certeza se isto é aceitável em seu ambiente.

Usando o RCPT TO

Este comando identifica o destinatário de uma mensagem de e-mail. Este comando pode ser usado diversas vezes para uma mensagem para entregar uma única mensagem a muitos destinatários. Veja um exemplo:

```
telnet 10.0.0.1 25
 220 server1 ESMTP Sendmail 8.9.3
 HELO
 501 HELO requires domain address
 HELO x
 250 server1 Hello [10.0.0.72], pleased to meet you
 MAIL FROM:link
```

```
250 link... Sender ok
RCPT TO:link
250 link... Recipient ok
RCPT TO: zelda
550 zelda... User unknown
```

Apesar destes ataques não serem difíceis de serem executados a partir de uma linha de comando, existem outras opções de ataques SMTP com o uso ferramentas como TamoSoft’s Essential NetTools ou NetScanTools Pro.

SMTP Relay

O serviço SMTP Relay deixa os usuários enviarem e-mails através de servidores externos. Relays de e-mails abertos não são um problema que costumavam ser, mas você ainda precisa checa-los. Spammers e hackers podem usar servidores de e-mail para enviar spam ou malwares através de e-mail disfarçado com um open-relay sem suspeitas.

Sugestões de livros: