Kiểm tra quá trình mã hóa email

Phân tích giao thức POP3, IMAP và SMTP thông qua cơ chế bảo mật SSL

Để thuận lợi cho quá trình phân tích này, sẽ rất tốt khi "nói chuyện" trực tiếp với server SMTP hoặc IMAP của bạn. Nhưng mọi việc sẽ trở nên phức tạp khi tiến hành mã hóa dữ liệu đầu cuối, nhưng với các công cụ thích hợp, việc này sẽ không quá khó khăn.

Thông thường, hầu như tất cả hệ thống mail server đều yêu cầu lựa chọn cơ chế mã hóa kết nối. 2 phương thức sau được sử dụng – hoặc toàn bộ các địa chỉ gửi qua SSL hoặc 1 cơ chế khác là StartTLS sẽ được sử dụng để kích hoạt quá trình mã hóa sau khi nhận được yêu cầu kết nối.

Trước tiên hãy xem qua về dịch vụ SSL, thường được sử dụng với các yêu cầu chuyên dụng, đặc biệt qua cổng TCP. Sau đây là bảng tham khảo về các cổng quan trọng khác:

Service	***Abbreviation***	***TCP port***
HTTP over SSL	https	443
IMAP over SSL	imaps	993
IRC over SSL	ircs	994
POP3 over SSL	pop3s	995
SMTP over SSL	ssmtp	465

Dịch vụ này sẽ lắng nghe yêu cầu từ cổng TCP, đặc biệt là những kết nối trực tiếp qua SSL, ví dụ những hệ thống email client nào không hỗ trợ SSL sẽ không thể giao tiếp với server IMAPS qua cổng 993. Một khi các dữ liệu và

thông số mã hóa đã được thực hiện, chúng sẽ được "cấp phép" và tạo ra 1 tunnel – đường hầm riêng biệt, thông qua đó, quá trình lưu chuyển dữ liệu được thực hiện trong thực tế. Dựa vào các sự kết hợp và các thành phần liên quan trong kết nối SSL, khi xảy ra bất kỳ sự cố nào, các công cụ hỗ trợ như telnet và netcat thường có xu hướng rút ngắn quá trình này lại.

Tiếp theo là 1 bước kiểm tra nho nhỏ với **OpenSSL**, có bao gồm 1 ví dụ SSL client nho nhỏ có thể được sử dụng để tạo kết nối tới dịch vụ SSL như *https://www.heise.de*:

$ openssl s_client -host www.heise.de -port 443
CONNECTED(00000003)
[...]

Certificate chain
0 s:/C=DE/ST=Niedersachsen/L=Hannover/O=Heise Zeitschriften Verlag GmbH Co KG/OU=Netzwerkadministration/OU=Terms of use at www.verisign.com/rpa (c)05/CN=www.heise.de
i:/O=VeriSign Trust Network/OU=VeriSign, Inc./OU=VeriSign International Server CA - Class 3/OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
1 s:/O=VeriSign Trust Network/OU=VeriSign, Inc./OU=VeriSign International Server CA - Class 3/OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
---
[...]

Các thông tin trên được cung cấp và chứng thực bởi openssl, cho phép chúng ta kiểm tra các chứng nhận khác đã được sử dụng. Nếu không làm như vậy, chẳng khác nào các nhà quản lý ở cửa sẵn và chờ đợi những cuộc tấn công theo kiểu man-in-the-middle. Về mặt kỹ thuật, những ai có thể sử dụng công

nghệ ettercap hoàn toàn có thể lấy được mật khẩu quản trị 1 cách đơn giản.

Tham số mã hóa và giải mã tín hiệu SSL client hoàn toàn "vô hình" – transparent, vì vậy người sử dụng có thể liên lạc trực tiếp đến server:

GET / HTTP/1.1
Host: www.heise.de
<return>
HTTP/1.1 302 Found
Date: Wed, 16 Sep 2009 10:24:44 GMT
Server: Apache/1.3.34
Location: http://www.heise.de/
[...]

Đăng nhập vào IMAPS

Quá trình này chỉ phức tạp hơn 1 chút:

$ openssl s_client -host imap.irgendwo.de -port 993
[...]
** OK IMAP4 Ready 0.0.0.0 0001f994*
1 Login user-ju secret
1 OK You are so in
2 LIST "" ""*
** LIST (\HasChildren) "." "INBOX"*
** LIST (\HasNoChildren) "." "INBOX.AV"*
[...]
2 OK Completed (0.130 secs 5171 calls)
3 logout
** BYE LOGOUT received*
3 OK Completed

Khi thực hiện xong bước này, đừng quên sắp xếp lại các số thứ tự tương ứng với câu lệnh IMAP trước đó. Đối với giao thức POP3 cũng tương tự như vậy,

chúng ta phải tự xác thực bên trong “đường hầm” SSL bằng câu lệnh USER và PASS POP3:

$ openssl s_client -host pop.irgendwo.de -port 995
[...]
+OK POP server ready H mimap3
USER user-ju
+OK password required for user "user-ju"
PASS secret
+OK mailbox "user-ju" has 0 messages (0 octets) H mimap3
quit
+OK POP server signing off

Đây có thể coi là sự lựa chọn và thay thế thích hợp dành cho công cụ telnet-ssl.

StartTLS

Những nhà cung cấp dịch vụ Internet đặc biệt thích sử dụng mô hình SSL, Transport Layer Security thông qua StartTLS. Mô hình này có lợi thế hơn với nhiều lựa chọn trong khi vẫn cho phép client không giao tiếp với server mà không được mã hóa. Mặt trái của điều này là các email client cần phải tương tác trực tiếp với server nếu muốn từ chối 1 kết nối TLS bất kỳ nào đó.

Lựa chọn mặc định của email client là "*TLS, if available*" đi kèm với sự mạo hiểm, các cuộc tấn công man-in-the-middle có thể “nhẹ nhàng” thay đổi câu lệnh StartTLS – với tính năng kích hoạt quá trình mã hóa, thành XtartTLS. Sau đó, server sẽ phản hồi lại rằng không thực hiện lệnh XtartTLS, và gây ra hiện tượng các email client khi gửi dữ liệu trong dạng chưa mã hóa vào 1 form không xác định ngược về phía người sử dụng. Do đó, khuyến cáo nên kiểm tra kỹ rằng máy chủ có thể xử lý lệnh StartTLS, và sau đó kích hoạt tính năng này. Nếu nhận được thông báo lỗi bất kỳ, rõ ràng là đã có vấn đề đâu đó trong hệ thống.

Các cổng mà dịch vụ TLS hoạt động trên đó phụ thuộc vào phía nhà cung cấp. Về nguyên tắc, các kiểu mã hóa này có thể nhúng 1 cách "vô hình" – transparent, vào trong hệ thống mà không yêu cầu bất kỳ hành động nào. Để tìm hiểu về hệ thống mail server có hỗ trợ tính năng này hay không:

$ nc smtp.irgendwo.de smtp
220 Mailserver ESMTP Exim 4.69 Wed, 16 Sep 2009 13:05:15 +0200
ehlo test
250-Mailserver Hello loki [10.1.2.73]
250-SIZE 78643200
250-PIPELINING
250-STARTTLS
250 HELP
quit
221 Mailserver closing connection

Danh sách này nên đi kèm với lệnh StartTLS, chức năng chính là kích hoạt quá trình mã hóa Transport Layer Security:

STARTTLS
220 TLS go ahead

Vào thời điểm này, Netcat sẽ gây ra 1 số phiền phức khó hiểu, nhưng OpenSSL lại có thể khắc phục điều này dễ dàng. Các nhà phát triển đã tạo ra hệ thống SSL client đủ thông minh để yêu cầu mã hóa TLS đối với các giao thức SMTP, POP3, IMAP và FTP, mặc dù không hoạt động với tất cả các server:

$ openssl s_client -host mail.irgendwo.de -port 25 -starttls smtp
CONNECTED(00000003)
[...]
250 HELP
ehlo test
250-Mailserver Hello loki [10.1.2.73]
250-SIZE 52428800

250-PIPELINING
250-AUTH PLAIN LOGIN
250 HELP

Cơ chế xác thực SMTP

Việc xác thực trong SMTP có 1 chút rắc rối hơn. Đối với hầu hết server, như trong ví dụ này, hỗ trợ phương thức AUTH PLAIN, nơi các dữ liệu phải đạt chuẩn Base64. Quá trình này được xử lý bởi câu lệnh Pearl sau:

$ perl -MMIME::Base64 -e 'print encode_base64("\000user-ju\000secret")'
AHVzZXItanUAc2VjcmV0

Kết quả thu được sẽ phải khớp với yêu cầu từ SMTP server:

AUTH PLAIN AHVzZXItanUAc2VjcmV0
235 Authentication succeeded

Những tín hiệu nhận được đã sẵn sàng với các các câu lệnh SMTP tiếp theo, đối với các địa chỉ và server không hỗ trợ OpenSSL, người sử dụng có thể dùng gnutls-cli có sẵn trong gói gnutls-bin. Đầu tiên, nó tạo ra 1 kết nối có dạng cleartext tới bất kỳ dịch vụ độc quyền TLS nào như:

$ gnutls-cli -s -p submission smtp.heise.de
Resolving 'smtp.heise.de'...
Connecting to '10.1.2.41:587'...

- Simple Client Mode:

220 taxis03.heise.de ESMTP Exim 4.69 Wed, 16 Sep 2009 18:03:01 +0200
ehlo test
250-taxis03.heise.de Hello loki.ct.heise.de [10.10.22.75]
250-SIZE 78643200
250-PIPELINING
250-STARTTLS

250 HELP
starttls
220 TLS go ahead

Tiếp theo, chuyển sang câu lệnh thứ 2 để xử lý ID của các công cụ và gửi trực tiếp tín hiệu SIGALARM tới đó:

$ ps aux | grep gnutls
ju 6103 pts/3 S+ 18:03 0:00 gnutls-cli [...]
$ kill -s SIGALRM 6103

Điều này sẽ khiến gnutls-cli dàn xếp với chuẩn TLS và tự động kết nối lại tham số ***stdin***và ***stdout*** để tạo ra "đường hầm" mới. Đồng thời, cũng chỉ ra 1 số thông tin khá thú vị về kết nối TLS mới tạo ra:

**** Starting TLS handshake*
- Certificate type: X.509
- Got a certificate list of 1 certificates.

- Certificate[0] info:
 # The hostname in the certificate matches 'smtp.heise.de'.
 # valid since: Thu Dec 14 14:08:41 CET 2006
 # expires at: Sun Dec 11 14:08:41 CET 2016
 # fingerprint: 28:8C:E0:29:B9:31:9B:96:F6:3D:B4:49:10:CD:06:80
 # Subject's DN: C=DE,ST=Niedersachsen,L=Hannover,O=Heise Zeitschriften Verlag GmbH Co KG,OU=Netzwerkadministration,CN=smtp.heise.de,EMAIL=admin@heise.de
 # Issuer's DN: C=DE,ST=Niedersachsen,L=Hannover,O=Verlag Heinz Heise GmbH & Co KG,OU=Netzwerkadministration,CN=admin@heise.de,EMAIL=admin@heise.de

- Peer's certificate issuer is unknown

- Peer's certificate is NOT trusted
- Version: TLS 1.0
- Key Exchange: DHE RSA
- Cipher: AES 256 CBC
- MAC: SHA
- Compression: NULL
quit
221 taxis03.heise.de closing connection
- Peer has closed the GNUTLS connection

Điều này cho phép người sử dụng kết nối trực tiếp đến thư viện lưu trữ các dịch vụ để kích hoạt TLS. Nếu người dùng muốn thử nghiệm thêm để chắc chắn rằng OpenSSL có hỗ trợ ***s_server*** để có thể thực thi các câu lệnh và gửi đến ***www*** server. Tính năng ***gnutls-serv*** đồng thời cũng cung cấp các chức năng tương đương ở trong gói ***gnutls-bin***.