

BÁO CÁO LAB 2: SCANNING NETWORK

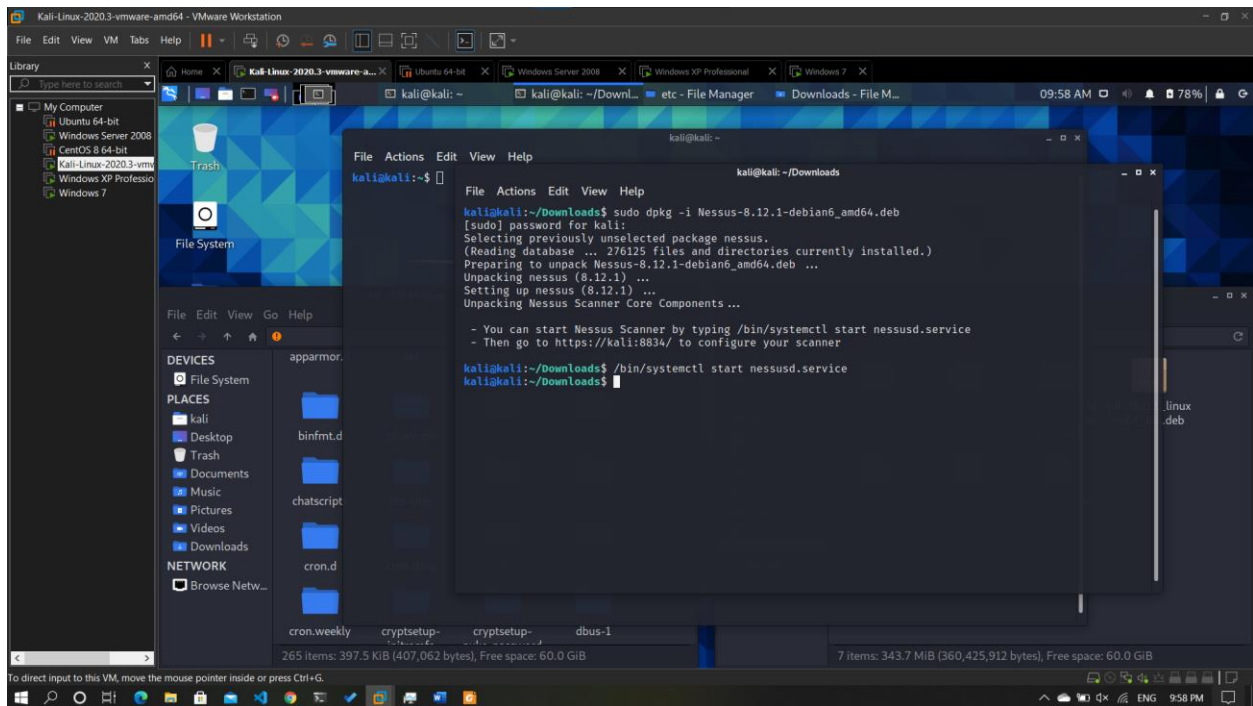
Môn học: An ninh máy tính

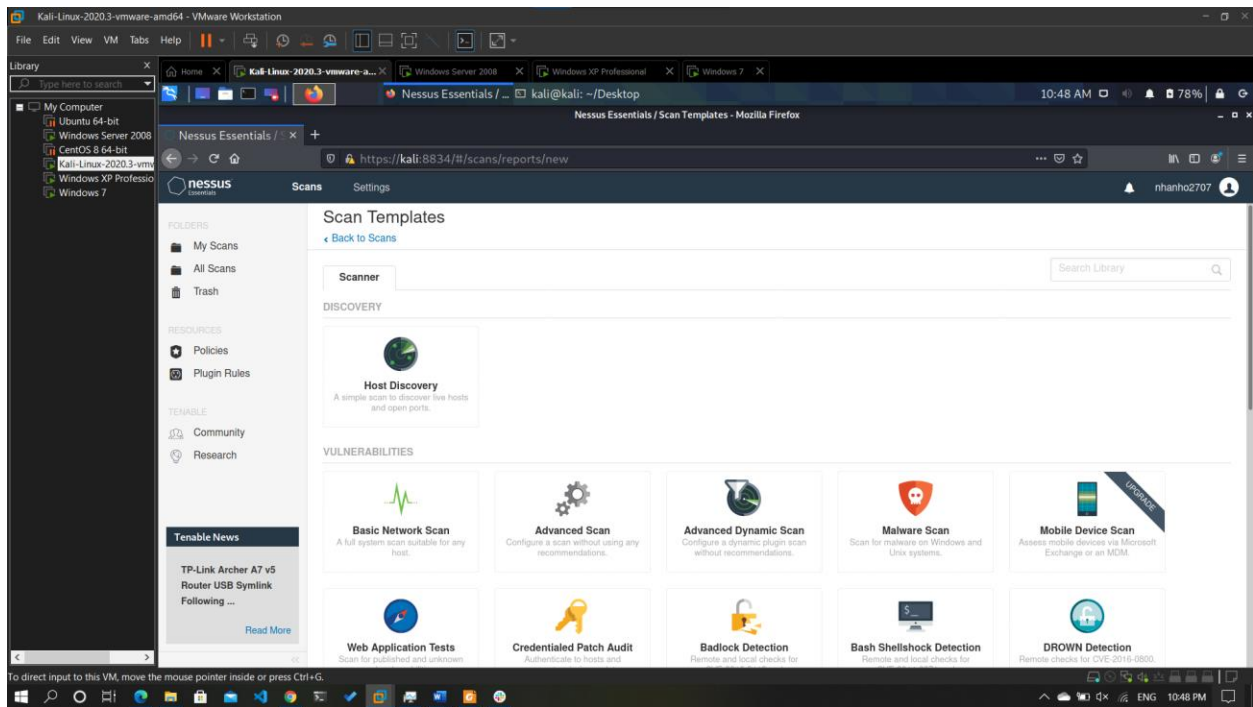
Họ và tên: Hồ Thanh Nhân

MSSV: 1712627

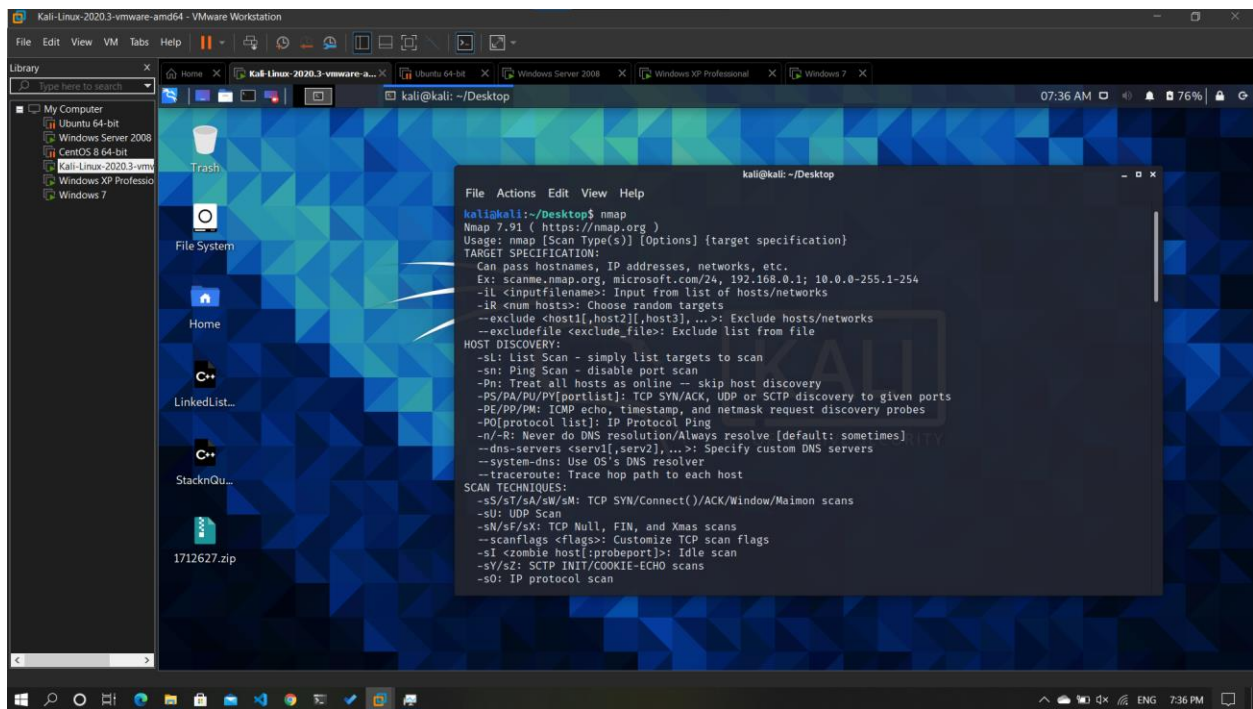
Câu 1:

Cài Nessus

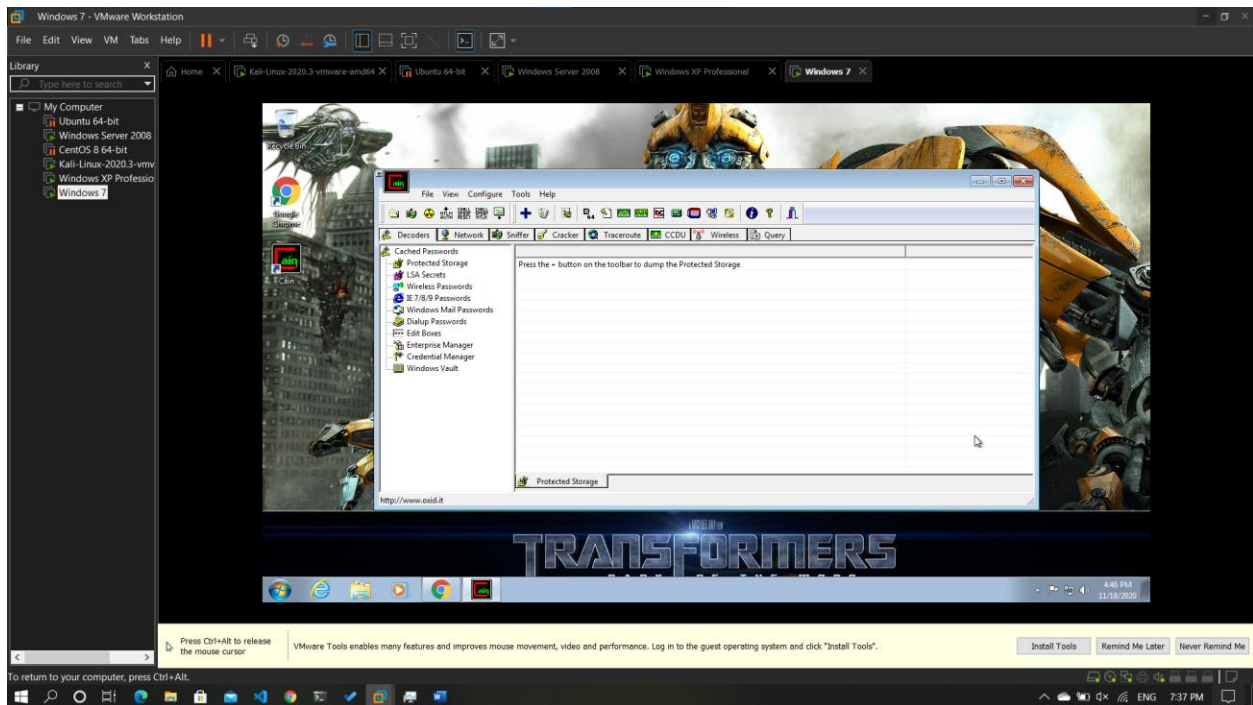




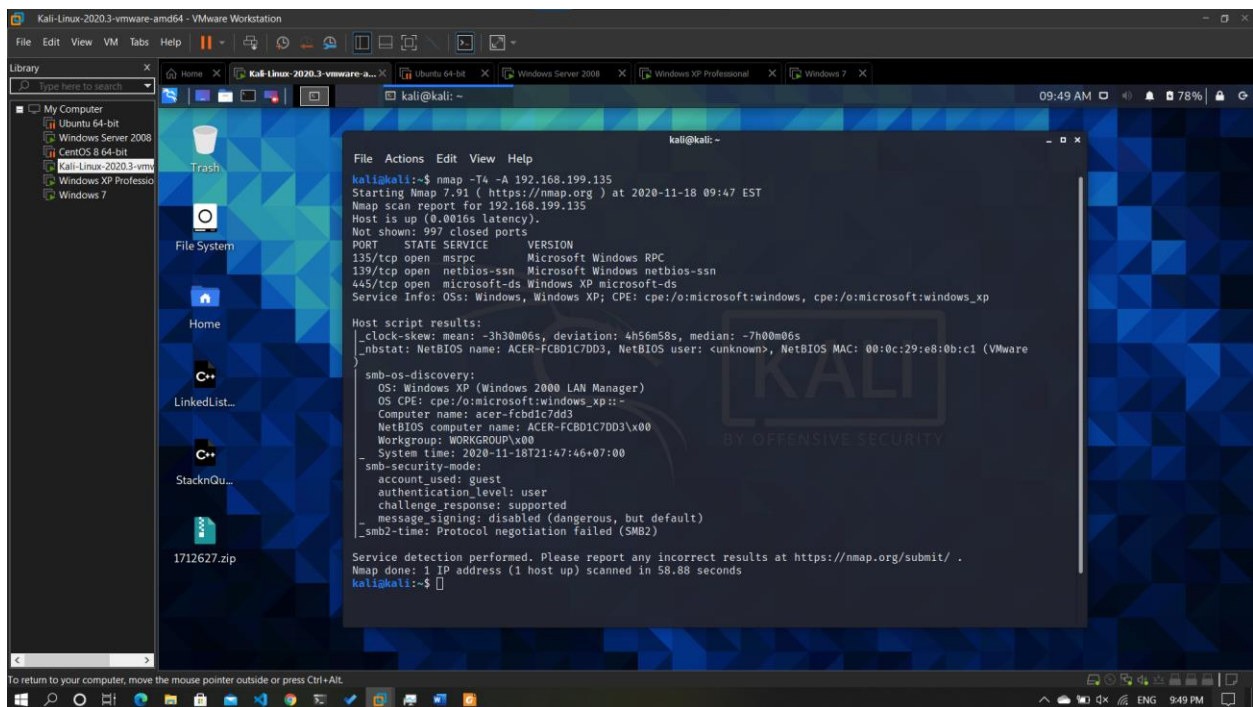
Nmap



Cain and Abel



Câu 2:



-Hệ điều hành Windows XP

- Port đang mở: 135, 139, 445

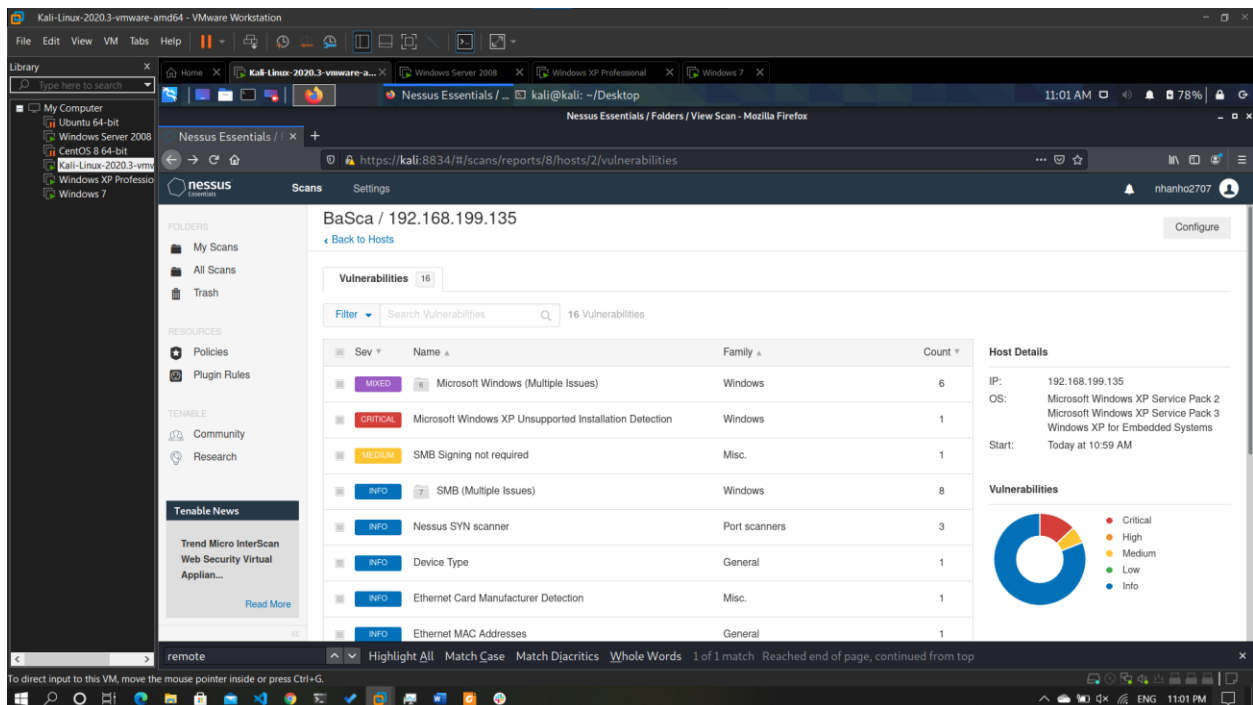
- Các dịch vụ tương ứng với port:

+ 135 msrpc: Microsoft Remote Procedure Call

- + 139 netbios-ssn: Network Basic Input/Output System Session service
- + 445 microsoft-ds: Microsoft Directory Services

Câu 3:

Sử dụng Nessus để quét lỗ hổng



BaSca / 192.168.199.135

[Back to Hosts](#)

Vulnerabilities: 16

Filter: Search Vulnerabilities 16 Vulnerabilities

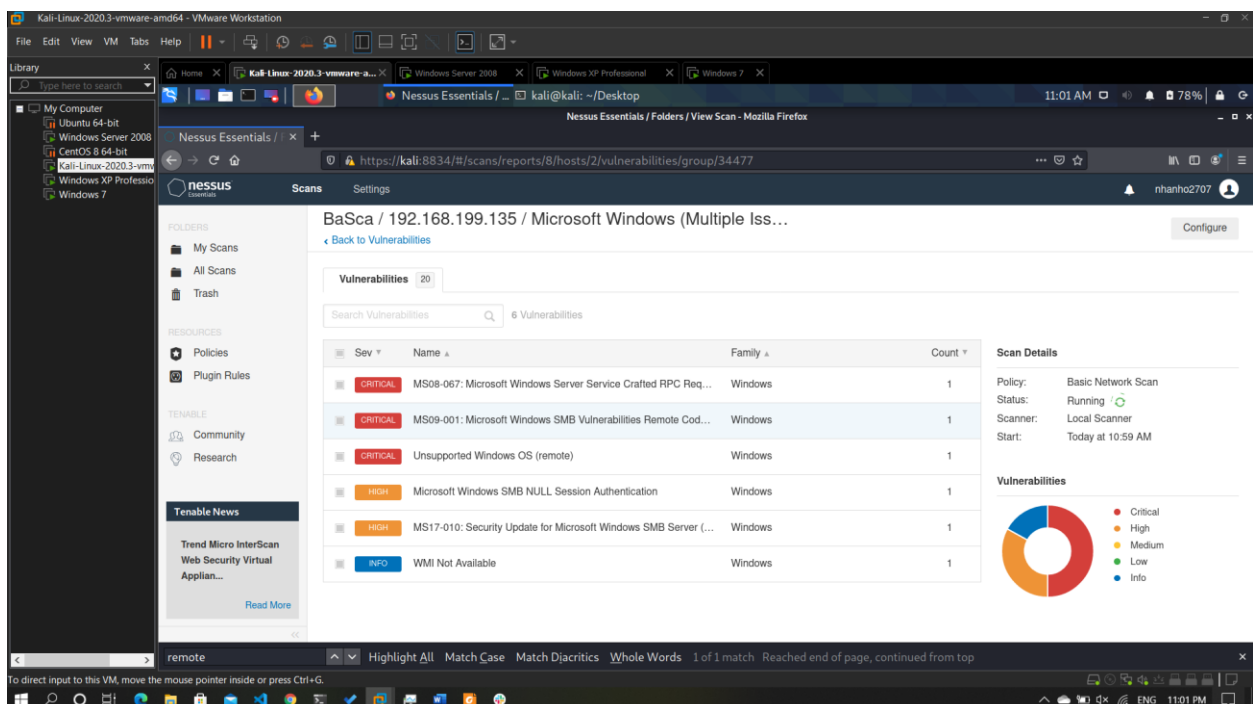
| Sev | Name | Family | Count |
|----------|---|---------------|-------|
| MIXED | Microsoft Windows (Multiple Issues) | Windows | 6 |
| CRITICAL | Microsoft Windows XP Unsupported Installation Detection | Windows | 1 |
| MEDIUM | SMB Signing not required | Misc. | 1 |
| INFO | SMB (Multiple Issues) | Windows | 8 |
| INFO | Nessus SYN scanner | Port scanners | 3 |
| INFO | Device Type | General | 1 |
| INFO | Ethernet Card Manufacturer Detection | Misc. | 1 |
| INFO | Ethernet MAC Addresses | General | 1 |

Host Details

IP: 192.168.199.135
 OS: Microsoft Windows XP Service Pack 2
 Microsoft Windows XP Service Pack 3
 Windows XP for Embedded Systems
 Start: Today at 10:59 AM

Vulnerabilities

Donut chart showing severity distribution: Critical (1), High (1), Medium (1), Low (8), Info (4).



BaSca / 192.168.199.135 / Microsoft Windows (Multiple Iss...

[Back to Vulnerabilities](#)

Vulnerabilities: 20

Search Vulnerabilities 6 Vulnerabilities

| Sev | Name | Family | Count |
|----------|--|---------|-------|
| CRITICAL | MS08-067: Microsoft Windows Server Service Crafted RPC Req... | Windows | 1 |
| CRITICAL | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Cod... | Windows | 1 |
| CRITICAL | Unsupported Windows OS (remote) | Windows | 1 |
| HIGH | Microsoft Windows SMB NULL Session Authentication | Windows | 1 |
| HIGH | MS17-010: Security Update for Microsoft Windows SMB Server (...) | Windows | 1 |
| INFO | WMI Not Available | Windows | 1 |

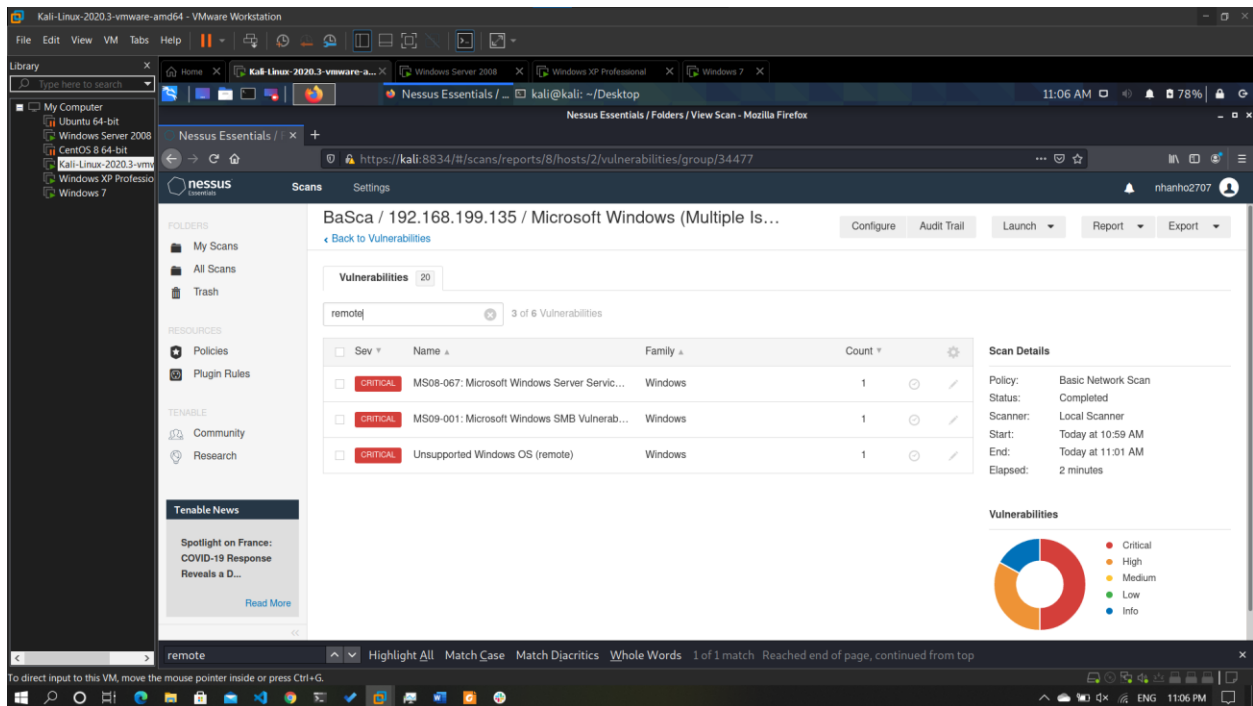
Scan Details

Policy: Basic Network Scan
 Status: Running
 Scanner: Local Scanner
 Start: Today at 10:59 AM

Vulnerabilities

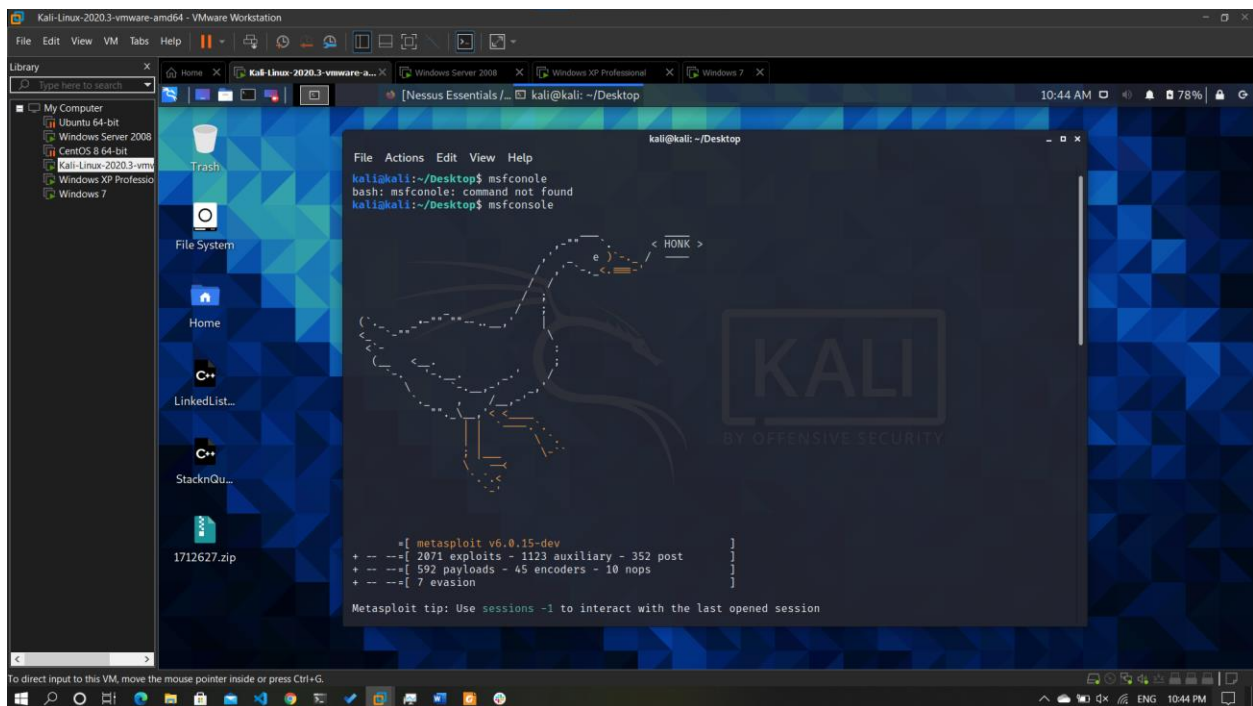
Donut chart showing severity distribution: Critical (3), High (2), Medium (1), Low (0), Info (0).

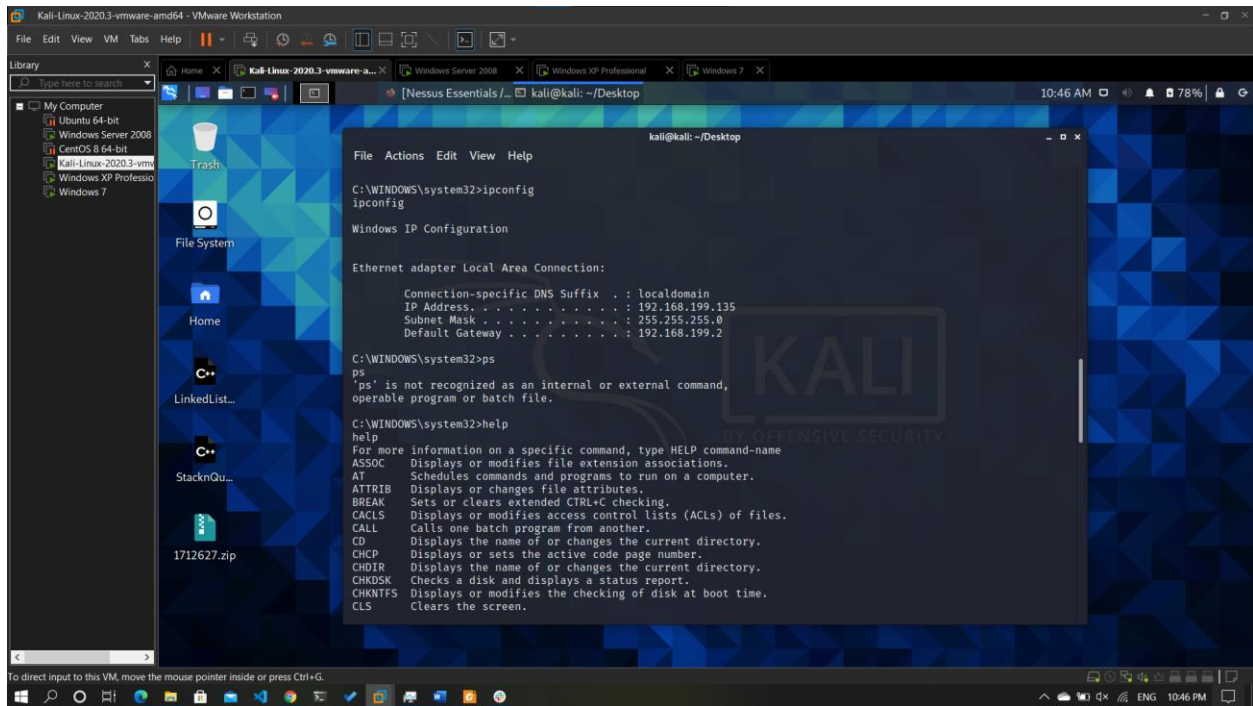
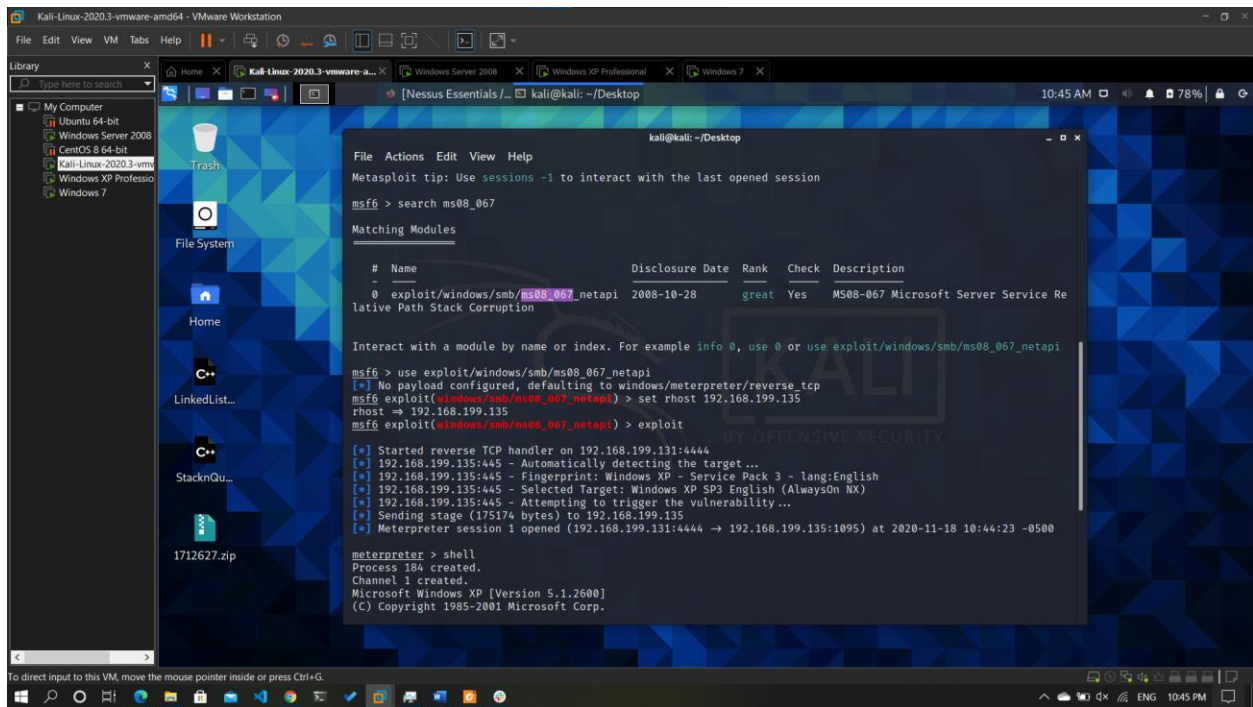
Các lỗ hổng truy cập từ xa:



Câu 4:

Sử dụng metasploit để khai thác lỗ hổng remote





Câu 5:

Cách khắc phục các lỗi hỏng:

- + Cập nhật phiên bản phần mềm mới nhất được hỗ trợ và vá lỗi bởi nhà phát triển
- + Đặt mật khẩu mạnh đủ bảo mật