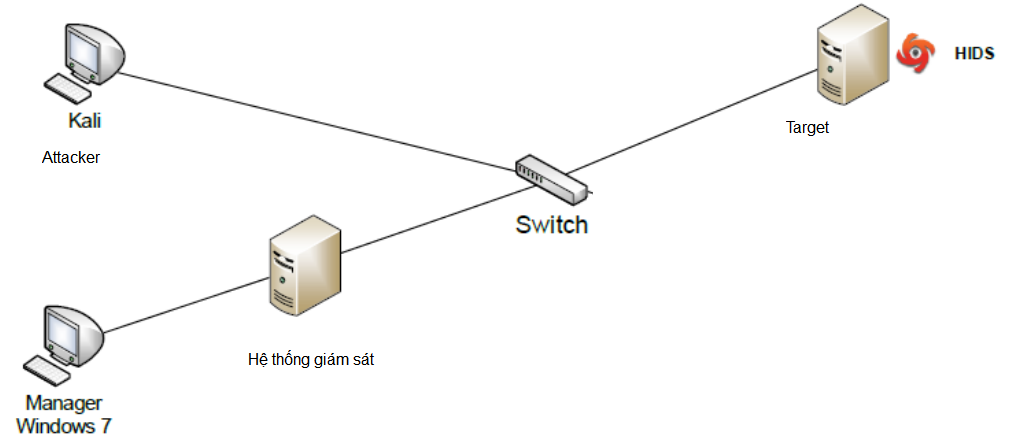
**Bài tập môn Giám sát và Ứng phó sự cố ATTT**

**Mô hình hệ thống**

****

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Giải pháp** | **Nhóm** | **Nhiệm vụ 1** | **Nhiệm vụ 2** | **Nhiệm vụ 3** | **Nhiệm vụ 4** |
| 1 | OSSEC | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 2 | OSSEC | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công từ chối dịch vụ (sử dụng slowloris) lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 3 | OSSEC | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu WinServer 2008 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 4 | Wazuh | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 5 | Wazuh | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công từ chối dịch vụ (sử dụng slowloris) lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 6 | Wazuh | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu WinServer 2008 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 7 | AlienVault | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 8 | AlienVault | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công từ chối dịch vụ (sử dụng slowloris) lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 9 | AlienVault | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu WinServer 2008 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 10 | Splunk | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 11 | Splunk | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công từ chối dịch vụ (sử dụng slowloris) lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 12 | Splunk | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu WinServer 2008 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 13 | ELK (Elasticsearch Logstash Kibana) | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 14 | ELK (Elasticsearch Logstash Kibana) | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công từ chối dịch vụ (sử dụng slowloris) lên máy mục tiêu Win7 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |
| 15 | ELK (Elasticsearch Logstash Kibana) | SV1:  SV2:  SV3:  SV4: | Cài đặt hệ thống | Thực hiện tấn công khai thác 01 lỗ hổng MS lên máy mục tiêu WinServer 2008 | Giải thích hoạt động của hệ thống giám sát khi có tấn công (tìm tập luật phát hiện tấn công, CSDL mã độc ....) | Nêu giải pháp ứng phó sự cố |