

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 04

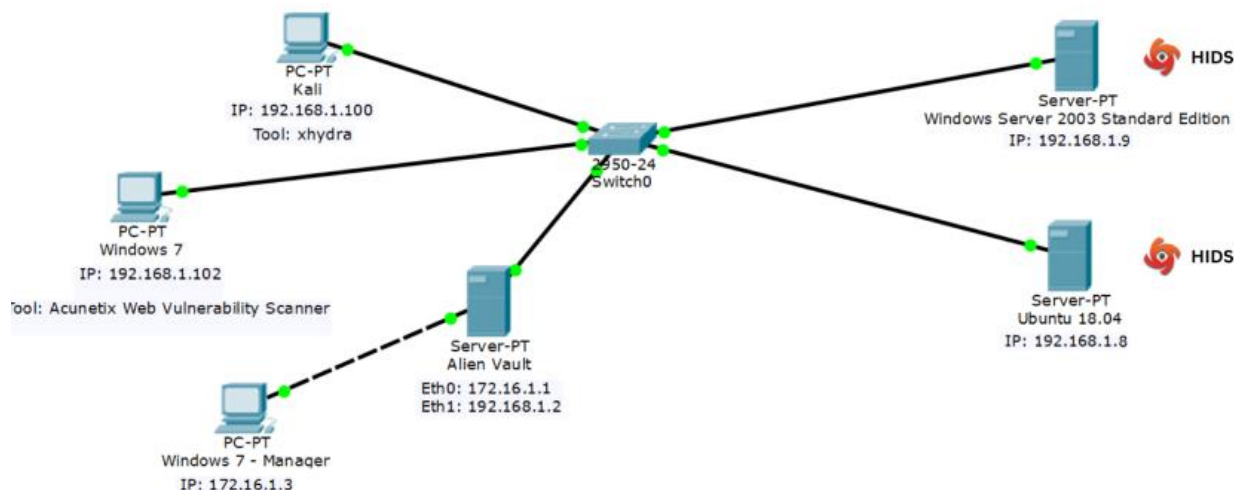
Triển khai hệ thống giám sát AlienVault

Sinh viên thực hiện:

Nguyễn Đức Mạnh - AT170432

1. CHUẨN BỊ

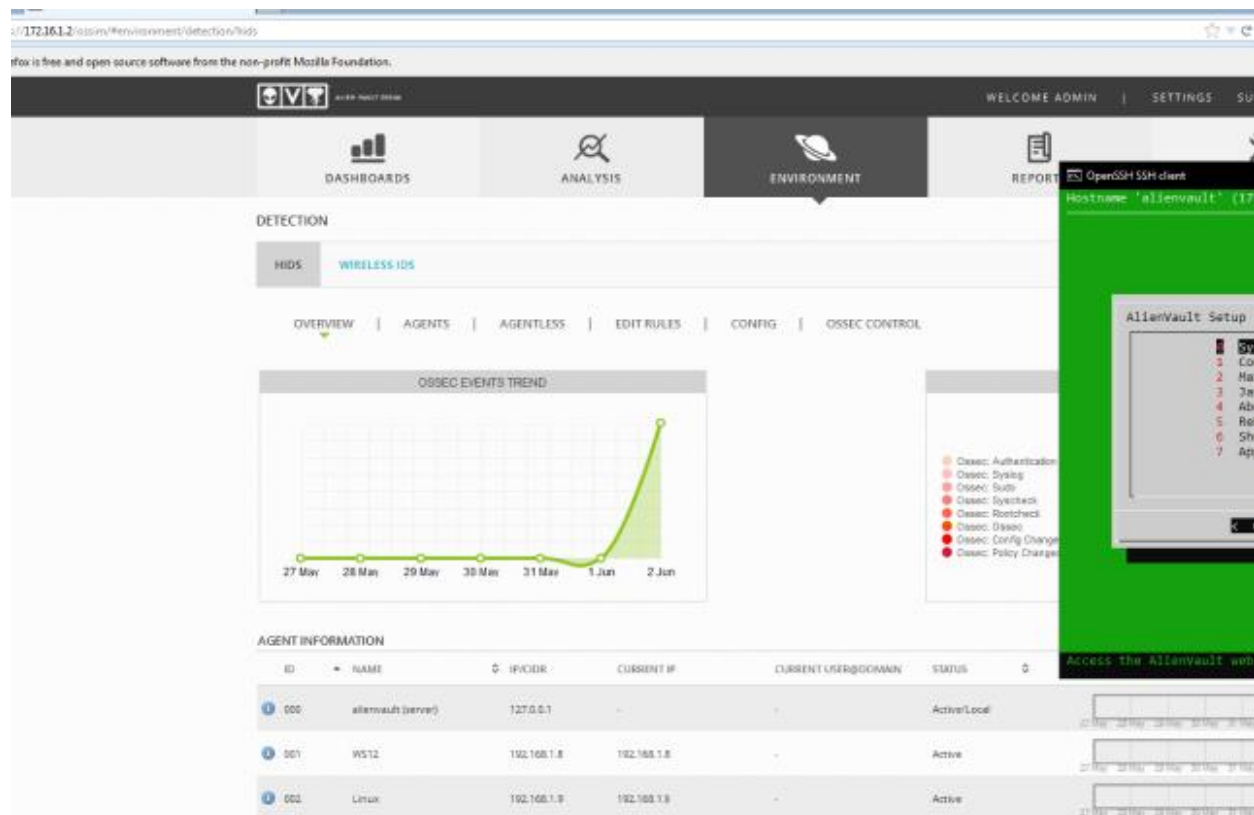
Vẽ lại mô hình mạng chuẩn bị thực hành (bao gồm các kết nối, địa chỉ IP, hệ điều hành, tên máy, ứng dụng được cài đặt)



2. THỰC HÀNH

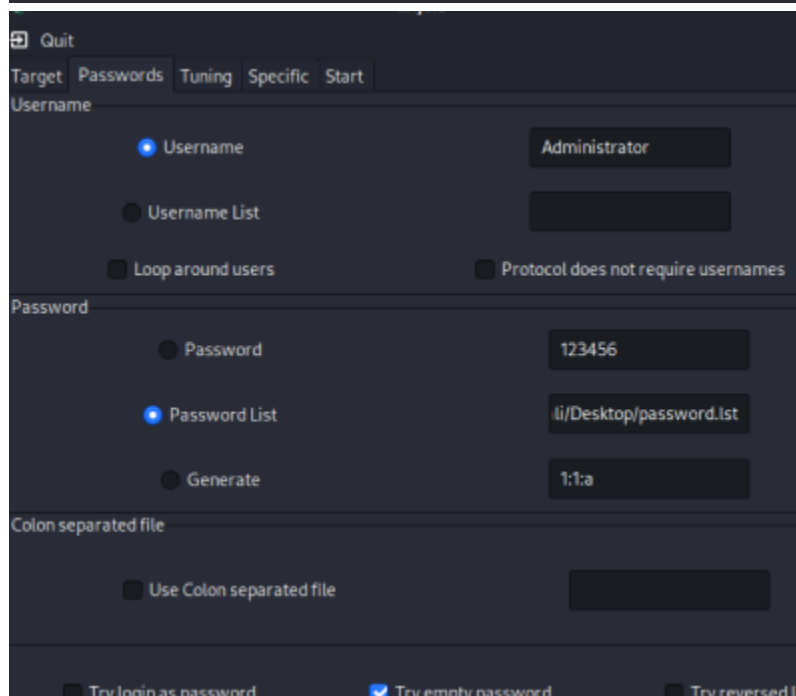
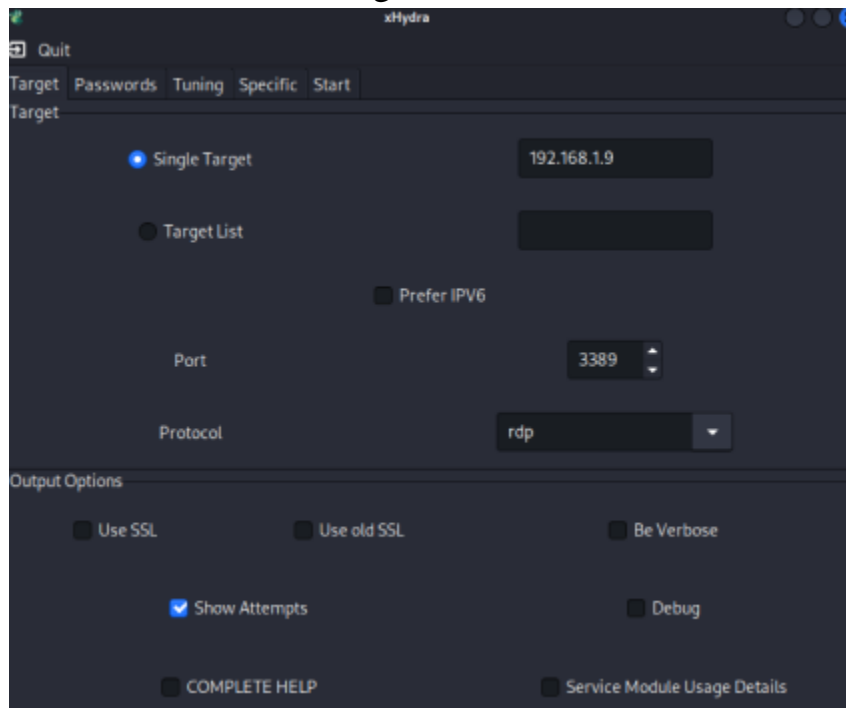
Kịch bản 1. Quản lý AlienVault qua giao diện Web

Chụp ảnh kết nối từ máy quản lý bằng trình duyệt Web tới máy chủ AlienVault và dán vào bên dưới.



Kịch bản 2. Thử nghiệm tấn công vào mật khẩu trên máy Server 2003

Thực hiện tấn công từ điển mật khẩu vào tài khoản Administrator



Kết quả

```
Hydra v9.4 (c) 2022 by van Hauser / THC & David Maciejak - Please do not use in  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-03 15:  
[WARNING] the rdp module is experimental. Please test, report - and if possible  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88399 login tries (l:1/p:88399)  
[DATA] attacking rdp://192.168.1.9:3389/  
[WARNING] The environment variable HYDRA_PROXY_CONNECT is not used!  
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to red  
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connection  
[ATTEMPT] target 192.168.1.9 - login "Administrator" - pass "" - 1 of 88399 [chi  
[ATTEMPT] target 192.168.1.9 - login "Administrator" - pass "!1234 " - 2 of 883  
[ATTEMPT] target 192.168.1.9 - login "Administrator" - pass "!aaa123" - 3 of 88  
[ATTEMPT] target 192.168.1.9 - login "Administrator" - pass "!aaa1234" - 4 of 8  
[3389][rdp] host: 192.168.1.9 login: Administrator password: !1234  
[3389][rdp] host: 192.168.1.9 login: Administrator password: !aaa1234  
[3389][rdp] host: 192.168.1.9 login: Administrator password: !aaa123  
[3389][rdp] host: 192.168.1.9 login: Administrator  
1 of 1 target successfully completed, 4 valid passwords found
```

Ảnh giao diện web quản trị AlienVault với chức năng giám sát thời gian thực, phát hiện sự kiện tấn công từ điện và dán vào bên dưới.

SIEM REAL-TIME						
PAUSE Done: [0 new rows]						
DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2023-06-03 16:33:00	ossec: Logon Failure - Unknown user or bad password.	0	ossec-win_authentication_failed	alienvault	0.0.0.0	192.168.1.9
2023-06-03 16:42:52	ossec: Logon Failure - Unknown user or bad password.	0	ossec-win_authentication_failed	alienvault	0.0.0.0	192.168.1.9

Kịch bản 3. Phát hiện tấn công quét lỗ hổng đối với mã nguồn website

Sử dụng công cụ Acunetix Web Vulnerability Scanner để quét lỗ hổng

Scan Results	Status
Scan Thread 1 (http://192.168.1.8)	Finished (6 alerts)
Web Alerts (6)	
OPTIONS method is enabled (1)	
Broken links (1)	
Error page Web Server version discl...	
Possible internal IP address disclosur...	
Knowledge Base (1)	
List of external hosts	
Site Structure	
/	OK
icons	Not Found
manual	Not Found
Variation 1 for user-agent	OK
Variation 2 for user-agent	OK
Cookies	

Kết quả

Alerts summary 6 alerts

Acunetix threat level
Level 1: Low

Acunetix Threat Level 1
One or more low-severity type vulnerabilities have been discovered by the scanner.

Total alerts found	
High	0
Medium	0
Low	1
Informational	5

Target information	http://192.168.1.8
Statistics	1053 requests
Progress	Scan is finished 100.00%