BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Lab 3: Simple Worm**

*GVHD: Trương Thị Hoàng Hảo*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.P21.ANTT.2

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Mai Xuân Huy | 22520553 | 22520553@gm.uit.edu.vn |
| 2 | Đào Xuân Vinh | 22521666 | 22521666@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 2 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**Link youtube:** [**Simple Worm**](https://www.youtube.com/watch?v=FK_1VyH8zsw)

**Soucre code:** [**GitHub**](https://github.com/SPRINGPEACHVINH/NT230.P21.ANTT/tree/main/Simpleworm)

1. **Môi trường**

* Gồm 3 máy
  + Attacker (Client)
    - IP: 192.168.42.143
  + Server
    - IP: 192.168.42.144
  + Victim (Client1)
    - IP: 192.168.42.128
* Mô hình: Server và Victim thuộc cùng mạng nội bộ, đã cấu hình ssh connection (Victim lưu pub key của Server). Attacker ngoài mạng.

1. **Kịch bản**

* Attacker khai thác remote buffer overflow khiến Server tạo reverse shell đến port 4444 của Attacker, sau đó chèn worm để quét mạng nội bộ của server, sau đó lây nhiễm worm đến máy Victim, worm trong máy Victim tiếp tục thực hiện quét mạng và lây nhiễm, khiến các máy bị nhiễm tự động thực thi ./vulserver 5000

1. **Luồng hoạt động**
2. Server chạy ./vulserver 5000
3. Attacker chạy file listener.py port 4444 để nhận reverse shell và auto tải worm, thực thi worm sau khi nhận tín hiệu reverse shell từ server
4. Attacker chạy remoteexploit <ip-server> 5000
5. Tạo thành công reverse shell, truy cập được shell của server
6. Worm được tải xuống server và chạy
7. Worm quét mạng của server tìm kiếm open host để gửi ./vulserver và worm
8. Worm tìm thấy Victim, lây nhiễm, cấp quyền file ./vulserver và worm.sh
9. Victim bị lây nhiễm, tự động thực thi ./vulserver và worm.sh, tiếp tục tìm các open host của Victim
10. Attacker chạy remoteexploit2 <ip-victim> 5000, đồng thời chạy listener.py port 4445
11. Khai thác thành công Victim, truy cập được shell thông qua port 4445
12. **Demo**
13. Code chính: remoteexploit.c, remoteexploit2.c, listener.py, worm.sh

* Remoteexploit.c được cấu hình với thông tin: ip 192.168.42.143 port 4444
* Remoteexploit2.c được cấu hình với thông tin: ip 192.168.42.143 port 4445
* Listener.py tạo kết nối giống khi chạy netcat để nghe port tự nhập. Khi nhận được tín hiệu của reverse shell, nó tạo kết nối và thực thi lệnh tải worm.sh về /tmp/, cấp quyền và thực thi worm.sh. Ngoài ra nó vẫn nhận lệnh được nhập từ attacker đến shell của máy nạn nhân như netcat. Khi nhận tín hiệu từ attacker nó cũng sẽ trả về output của shell, giúp theo dõi quá trình lây nhiễm
* Worm.sh thực hiện quét dải mạng từ 1 – 256, cho sẵn mảng Username=(ubuntu, server, victim, client) để thử đăng nhập ssh vào các IP up. Khi ssh thành công, thực hiện lệnh cop file vulserver và worm từ máy đã bị lây nhiễm sang /tmp/ của máy victim vừa được phát hiện, sau đó cấp quyền và thực thi 2 file này trên các tiến trình khác nhau để giữ kết nối.

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure . remoteexploit.c

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure . remoteexploit2.c

A screen shot of a computer program

AI-generated content may be incorrect.

Figure . listener.py

A screen shot of a computer program

AI-generated content may be incorrect.

Figure . worm.sh

1. Hình ảnh chạy

* Cấu hình ssh connection cho server và victim

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

----Demo worm

* Server ./vulserver 5000

A black background with white text

AI-generated content may be incorrect.

* Attacker terminal 2: listener.py port 4444

A black screen with white text

AI-generated content may be incorrect.

* Sau khi Attacker gửi exploit đến server, listener.py 4444 đã nhận được reverse shell và gửi command tải worm, thực thi worm

A screen shot of a computer

AI-generated content may be incorrect.

* Thư mục /tmp/ của server trước và sau khi exploit

A black background with blue text

AI-generated content may be incorrect.

* Quá trình tải worm và thực thi của worm trên server

A screenshot of a computer

AI-generated content may be incorrect.

* Tìm thấy và kết nối được Victim

A screenshot of a computer error

AI-generated content may be incorrect.

* Thư mục /tmp/ của victim trước và sau khi bị lây nhiễm

A screenshot of a computer

AI-generated content may be incorrect.

* Telnet thành công tới Victim

A screen shot of a computer

AI-generated content may be incorrect.

* Attacker chạy listener.py port 4445 để nhận reverse shell của Victim

A black background with white text

AI-generated content may be incorrect.

* Attacker gửi remoteexploit2 đến Victim



* Nhận được reverse shell của Victim, trong reverse shell cũng cho thấy worm được tải và auto thực thi để lây nhiễm tiếp

A screenshot of a computer

AI-generated content may be incorrect.

---

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)