LAB 4

Khai thác tường lửa  
trong Linux  
Linux Firewall Exploration

BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 04 (Session 04)**

**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

Note: Vì một số lý do trong mạng nhà nên IP address được đổi lại để thuận tiện làm lab.

|  |  |  |
| --- | --- | --- |
| **Máy ảo** | **Interfaces** | **Thông tin** |
| Firewall | NAT  192.168.1.5/24 | Cài đặt pfSense (hướng dẫn trong phần 1 – Nội dung thực hành) sử dụng 2 card mạng: Card NAT: dùng để kết nối ra internet; Card Host Only: để kết nối đến VM A |
| HO  172.16.88.254/24 |
| VM A | HO  172.16.88.10 | Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng Host Only để kết nối đến máy Firewall. |
| VM B | NAT  192.168.1.10 | Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng NAT để kết nối đến Internet. Cài đặt thêm telnetd và ssh (server). |

*1. Không cho phép các máy trong mạng nội bộ (172.16.88.0/24) thực hiện ping đến  
máy VM B.*



*2. Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao  
thức http (cổng 80)*



*3. Chặn kết nối telnet từ mạng nội bộ ra bên ngoài.*



*4. Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và  
youtube.com*

### *Dùng SquidGuard Filter Package*

Graphical user interface, text, application, chat or text message

Description automatically generated

*Add vào “Deny”*

*5. Trình bày ý nghĩa các tham số sử dụng trong 2 lệnh thiết lập tunnel và kết nối  
telnet ở trên.*

***-f :*** *Yêu cầu ssh chuyển sang nền ngay trước khi thực hiện lệnh. Điều này rất hữu ích nếu ssh định yêu cầu mật khẩu hoặc cụm mật khẩu, nhưng người dùng muốn nó ở chế độ nền. Điều này ngụ ý -n. Cách được khuyến nghị để khởi động các chương trình X11(X-Windows) tại một trang web từ xa là sử dụng một thứ gì đó như ssh -f host xterm.*

***-N:*** *Không thực hiện lệnh từ xa, tốt trong trường hợp dùng forwarding port*

***-L:*** *Chỉ định rằng cổng đã cho trên máy chủ cục bộ (máy khách) sẽ được chuyển tiếp đến máy chủ đã cho và cổng ở phía từ xa. Điều này hoạt động bằng cách cấp phát một socket để lắng nghe cổng ở phía cục bộ, được liên kết tùy chọn với bind\_address được chỉ định. Bất cứ khi nào kết nối được thực hiện với cổng này, kết nối sẽ được chuyển tiếp qua kênh bảo mật và kết nối được thực hiện với cổng máy chủ lưu trữ của cổng từ máy tính từ xa. Chuyển tiếp cổng cũng có thể được chỉ định trong tệp cấu hình. Địa chỉ IPv6 có thể được chỉ định bằng cú pháp thay thế:*

*[bind\_address /] port / host / hostport hoặc bằng cách đặt địa chỉ trong dấu ngoặc vuông. Chỉ superuser mới có thể chuyển tiếp các cổng đặc quyền. Theo mặc định, cổng cục bộ được ràng buộc theo cài đặt GatewayPorts. Tuy nhiên, một bind\_address rõ ràng có thể được sử dụng để liên kết kết nối với một địa chỉ cụ thể. Bind\_address của '' localhost '' chỉ ra rằng cổng lắng nghe chỉ được sử dụng cục bộ, trong khi địa chỉ trống hoặc '\*' cho biết rằng cổng phải có sẵn từ tất cả các giao diện.*

*6. Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không?  
Nếu có, nguyên nhân tại sao Firewall không việc sử dụng telnet này? Nếu không,  
thì kết nối từ máy A đến máy B như thế nào để không đi qua máy Firewall?*

*Các gói tin này vẫn đi qua máy Firewall. Mặc định thì Firewall chặn các inbound telnet ra ngoài, nó đóng vai trò thực hiện chức năng kiểm soát và forward các gói tin, việc telnet giữa client-client là riêng và Firewall không can thiệp.*

*Kết nối từ máy A->B không qua Firewall thì dùng mapping port, ngầm định là vượt qua được Firewall*

*7. Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.*

*Tạo SSH Tunneling, thay port vì port 9000 đã bị dùng (do lần chạy trước)*

Text

Description automatically generated

*Vào facebook.com*

Graphical user interface, application

Description automatically generated

*8. Thực hiện ngắt SSH Tunnel, xoá cache của trình duyệt và truy cập lại trang*

*www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?*

*Trang web bị ngắt, không thể truy cập*

*9. Nếu trên Firewall, áp dụng rule chặn kết nối SSH (port 22), lúc này có thể thiết lập*

*tunnel này được hay không? Tại sao?*

*Lúc này bất kỳ gói tin nào có protocol là SSH đều bị block nên không thể thiết lập tunnel*

*10. Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát*

*của Firewall trong trường hợp trên*

*- Ngăn chặn các kết nối ssh outbound, do đó, bất kỳ tunnel nào sẽ yêu cầu phong tỏa hoàn toàn các kết nối gửi đi thông qua kiểm tra gói tin sâu. Nhìn vào các port sẽ vô dụng, phải nhìn vào packet thực tế để biết đó là SSH.*

*- Cách khác là cấu hình để ngăn chặn SSH Tunneling trên proxy*

*11. Đoạn chương trình script.pl trên hoạt động như thế nào?*

*12. Thay đổi nội dung đoạn chương trình trên để khi truy cập vào website  
example.com, một hình ảnh cảnh báo dừng lại xuất hiện (như hình dưới).*

*13. Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều  
được thay bằng hình ảnh bạn thích (như hình minh hoạ dưới)*

*14. Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức  
này có đặc điểm gì khác nhau?*

|  |  |  |  |
| --- | --- | --- | --- |
| ***L2TP*** | ***IPSec*** | ***OpenVPN*** | ***WireGuard*** |
| *Thuật toán mã hóa 3DES hoặc AES. Khóa 256 bit sẽ được sử dụng để mã hóa. Giao thức OpenVPN sử dụng mật mã AES với mã hóa 128bit và 256bit (Tùy chọn), thuật toán băm là 160bit SHA1, kênh điều khiển là TLSv1 / SSLv3 DHE-RSA-AES256-SHA và 2048 bit RSA.* | *IKEv2 triển khai một số lượng lớn các thuật toán mật mã bao gồm 3DES, AES, Blowfish, Camellia. IVPN triển khai IKEv2 bằng AES với các khóa 256 bit.* | *OpenVPN sử dụng thư viện OpenSSL để cung cấp mã hóa. OpenSSL thực hiện một số lượng lớn các thuật toán mật mã như 3DES, AES, RC5, Blowfish.*  *Như với IKEv2, IVPN triển khai AES với các khóa 256 bit.* | *Được xây dựng trên đỉnh ChaCha20 để mã hóa đối xứng (RFC7539), Curve25519 cho thỏa thuận khóa ẩn danh Elliptic-curve Diffie – Hellman (ECDH), BLAKE2s để băm (RFC7693), SipHash24 cho khóa băm và HKDF để lấy khóa (RFC5869). Sử dụng bắt tay dựa trên UDP và trao đổi khóa sử dụng bí mật chuyển tiếp hoàn hảo trong khi tránh cả các cuộc tấn công mạo danh xâm nhập và phát lại khóa.* |
| *Giao thức đường hầm lớp hai (L2TP) sử dụng cổng UDP 1701 và là một phần mở rộng của Giao thức đường hầm điểm-điểm. L2TP thường được sử dụng với IPSec để thiết lập Mạng riêng ảo (VPN)* | *IKEv2 sử dụng UDP 500 cho trao đổi khóa ban đầu, giao thức 50 cho dữ liệu được mã hóa IPSEC (ESP) và UDP 4500 cho truyền qua NAT.*  *IKEv2 dễ bị chặn hơn OpenVPN do sự phụ thuộc vào các giao thức và cổng cố định.* | *OpenVPN có thể dễ dàng được định cấu hình để chạy trên bất kỳ cổng nào bằng cách sử dụng UDP hoặc TCP, do đó dễ dàng vượt qua các bức tường lửa hạn chế.* | *WireGuard® sử dụng giao thức UDP và có thể được định cấu hình để sử dụng bất kỳ cổng nào. Có thể không chịu được việc định hình lưu lượng dễ dàng hơn OpenVPN do thiếu hỗ trợ cho TCP.* |

*15. Tìm hiểu và thực hiện cấu hình trên pfSense, sao cho từ máy VM B có thể mở kết  
nối VPN đến pfSense server để truy cập được máy VM A.*