Câu 1: Lập bảng tổng hợp các phương pháp tấn công mạng không dây (tên gọi, phương pháp thực hiện, công cụ sử dụng, kết quả thu được, biện pháp phòng chống…).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên tấn công | Phương pháp thực hiện | Công cụ sử dụng | Kết quả thu được | Biện pháp phòng chống |
| Wifi Discovery | Dò tìm và xác định các mạng Wifi có sẵn trong phạm vi | WiFi scanners (inSSIDer, NetSpot, Wi-Fi Analyzer) | Danh sách các mạng WiFi có sẵn, thông tin về kênh và tần số | Ẩn tên mạng (SSID), sử dụng WPA3, tăng cường bảo mật |
| GPS Mapping | Sử dụng GPS để ánh xạ vị trí của các điểm truy cập Wifi và mạng không dây xung quanh | GPS receivers, Mapping software | Bản đồ vị trí các điểm truy cập WiFi | Tắt chia sẻ vị trí, sử dụng VPN, tăng cường bảo mật |
| Wireless Traffic Analysis | Phân tích giao thông mạng không dây để thu thập thông tin | Wireshark, Tcpdump, Airodump-ng | Dữ liệu giao thông mạng, thông tin về thiết bị kết nối | Sử dụng mã hóa mạnh, giám sát và phát hiện xâm nhập (IDS/IPS) |
| Launch Wireless Attacks | Tấn công trực tiếp vào mạng không dây để kiểm thử bảo mật | Aircrack-ng, Fern Wifi Cracker, Fluxion | Kiểm thử bảo mật, đánh cắp thông tin đăng nhập, ngăn chặn kết nối | Sử dụng mã hóa mạnh, cập nhật hệ thống, theo dõi hoạt động mạng |
| Crack Wifi Encryption | Tấn công để phá mật khẩu mạng Wifi | Aircrack-ng, Hashcat, Reaver | Thu được mật khẩu WiFi và xâm nhập mạng | Sử dụng WPA3, mật khẩu mạnh, cập nhật firmware |

Câu 3: So sánh 3 phần mềm tường lửa phổ biến hiện nay.

|  |  |  |  |
| --- | --- | --- | --- |
| Tên phần mềm | FortiGate | Palo Alto Networks | SonicWall |
| Khả năng bảo mật | IPS đa động cơ, AV dựa trên đám mây, WAF đa lớp, chống thư rác và lừa đảo, kiểm soát truy cập chi tiết, sandboxing | IPS dựa trên hành vi và rủi ro, NGFW tích hợp, sandbox phân tích mối đe dọa, ngăn chặn tấn công lừa đảo và zero-day, tường lửa ứng dụng web (WAAS) | IPS Stateful, AV theo thời gian thực, WAF dựa trên danh sách, chống thư rác và spam, tường lửa dựa trên danh sách ACL, quản lý USB an toàn |
| Tính năng | VPN site-to-site và IPSec, quản lý băng thông, cân bằng tải, tường lửa ảo, báo cáo chi tiết, tích hợp SIEM | IPSec VPN tiên tiến, tường lửa phân đoạn (micro-segmentation), phân tích lưu lượng theo chủ đề, tường lửa DNS, tự động hóa quy trình bảo mật (SOAR) | VPN SSL và IPSec, quản lý chất lượng dịch vụ (QoS), cân bằng tải WAN, Wi-Fi bảo mật, quản lý thiết bị di động (MDM), sao lưu và khôi phục dữ liệu |
| Hiệu suất | Xử lý lưu lượng cao, độ trễ thấp, hiệu suất VPN mạnh mẽ, tài nguyên hệ thống tối ưu | Hiệu suất cao với các tác vụ bảo mật sâu, xử lý mã hóa SSL, khả năng mở rộng linh hoạt | Hiệu suất ổn định cho các doanh nghiệp vừa và nhỏ, cân bằng tốt giữa bảo mật và tốc độ, tùy chọn phần cứng chuyên dụng |
| Dễ sử dụng | Giao diện web trực quan, cấu hình đơn giản, hướng dẫn từng bước, tài liệu phong phú | Giao diện web thân thiện, cấu hình nâng cao tùy chỉnh, tự động hóa quy trình, yêu cầu chuyên môn cao hơn | Giao diện web dễ dùng, cấu hình sẵn các mẫu chính sách, quản lý tập trung, hỗ trợ từ xa |
| Chi phí | Chi phí bản quyền cao, tùy theo model và tính năng, chi phí bảo trì có thể cao | Chi phí bản quyền cao nhất trong 3 phần mềm, tùy theo model và tính năng, chi phí bảo trì cao do yêu cầu chuyên môn cao | Chi phí bản quyền hợp lý, tùy theo model và tính năng, chi phí bảo trì thấp hơn |