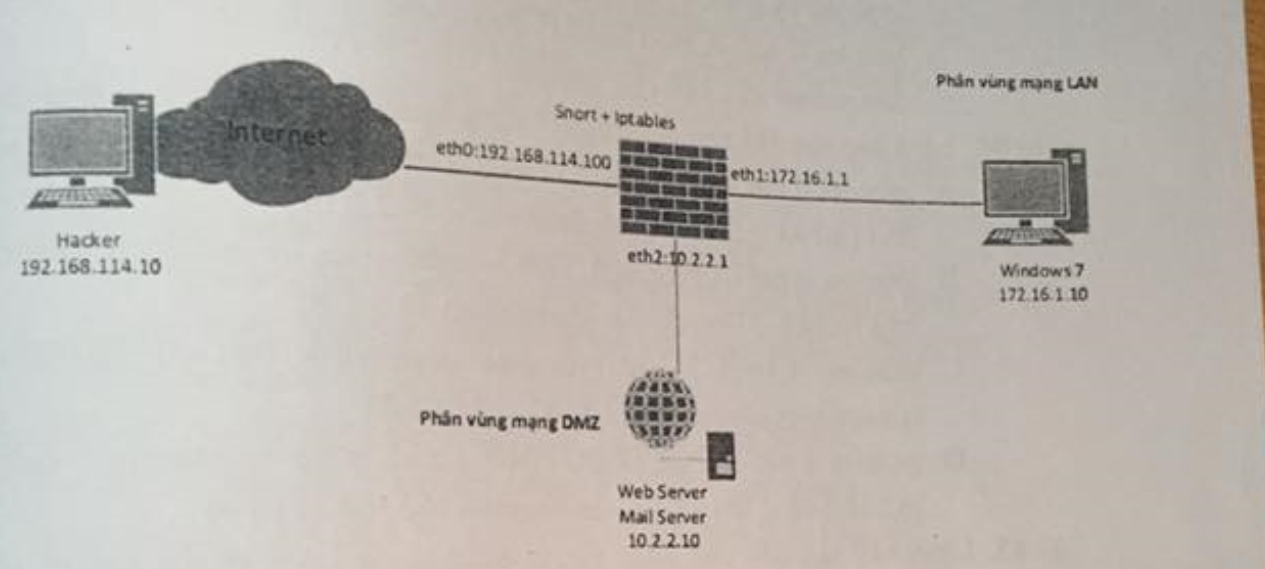
1. ổ cứng chạy hết công suất => virus đang phát tán.
2. Bộ lọc gói tin => chặn gói tin trái phép từ ngoài vào.
3. T bị lưu trữ inf đường dẫn trong mạng =>router
4. G thức sd nhiều, truyền tải, sd pp quay số trên internet =>SLIP
5. G thức ko phải đg hầm nhưng sd g thức dg hầm bảo mật =>IPSEC
6. Socket = IP+ port number
7. T bị giám sát mạng thụ động : Sniffer
8. Nhận mail từ microsoft + file kèm chạy => xóa mail
9. Hệ mật DES sd khối khóa = 56 bít ngẫu nhiên + 8 bit ktra
10. Hệ mật DES xử lý từng khối plaintext có độ dài = 64 bit
11. T toán SHA là => hàm băm 1 chiều+tạo chữ kí số+ giá trị băm = 160 bit
12. DSA là giải thuật => tạo chữ kí số (DS)
13. MD5 giá trị băm = 128 bit
14. Hệ mật RSA (p=5,q=7) =>khóa (e=7,d=23)
15. Diff-hellman dùng để => phân phối khóa trc cho hệ mật đối xứng
16. MAC viết tắt của => mã xác thực thông báo (message authentication code)
17. Pp bảo mật ko cần sd mật mã => điều khiển truy cập
18. K niệm ko chối bỏ khi gửi thông điệp => tính ko từ chối
19. Qtr mã hóa sd 1 khóa mã ở 2 phía của 1 phiên lm việc =>symmetrical
20. PKCS sd cặp khóa mã hóa =>public/private
21. Vấn đề nảy sinh khi sd sinh khóa mã tập trung =>truyền khóa
22. G thức cung cấp bảo mật đầu cuối UNIX từ xa =>SSH
23. Qtr xđ topology of mạng => quét mạng
24. Qtr chiếm quyền truy cập đến tài nguyên mạng => liệt kê
25. Qtr xđ vị trí và các inf mạng =>in dấu chân
26. Đảm bảo ATTT = bí mật + toàn vẹn + sẵn sàng
27. Đảm báo tính bí mật : ko có thẩm quyền thì ko đk truy cập
28. Đảm bảo tính toàn vẹn : giữ cho inf ko bị sửa đổi từ nơi phát đến nhận
29. ISO 27001:2013 ảnh hưởng tới ATTT =>ng, qtr- thủ tục,c sách,công nghệ
30. Rủi ro của HT TT tỷ lệ thuận với: nguy cơ mất ATTT + điểm yếu of hệ thống
31. Giảm nhẹ rủi ro HTTT cần: loại trừ các điểm yếu bảo mật của HT
32. Các pp q lý rủi ro ATTT : giảm nhẹ và loại trừ+ chuyển giao+chấp nhận rủi ro
33. ‘information security event’ => các sự kiện vi phạm cs ATTT,..
34. ‘information security accident’ => a hay chuỗi s kiện an ninh TT ko mong muốn,..
35. ISO 17799 – 2005 ATTT có bn lĩnh vực cần kiểm soát =>11
36. Pm qly cập nhật bản vá của Microsoft(WSUS 3.0) cập nhật bản á cho hđh => Window Vista
37. C năng of pm q lý, cập nhật bản vá Microsoft => cập nhật bản vá cho Windows
38. Pm qly cập nhật bản vá (WSUS 3.0) can cđ trên hdh nào?=>windows server 2003 sẻvices pack 1
39. WSUS 3.0 cập nhật những loại bản vá=>critical updates+ security+services updates
40. WSUS 3.0 bản vá cho HĐH 64 bit=> windows server 2008x64
41. L2TP xác thực ng dùng = p thức =>CHAP
42. Ưu điểm của L2TP(chọn 3) =>L2TP ksoát xác thực user,nhanh hơn ppp, nâng cao bảo mật nhờ TPSEC
43. TP SEC chạy ở **lớp 3** + sd IKE thiết lập SA
44. Ưu điểm of L2F => độc lập vs nền+đg hầm trên L2F nhanh hơn so vs PPTP
45. PPTP đưa ra dvu bảo mật: mã hóa và nén data + xác thực+ksoat và lọc gói tin
46. PPP lm việc ở **tầng Lkết data** trong mô hình OSI
47. PPTP sd PPP thực hiện thiết lập, finish vật lý,xđ user,tạo gói data => sai
48. Cơ chế xác thực sd bởi PPTP => bắt tay CHAP
49. Các t bị bảo mật ko phải IDS => cả 3 ABC
50. C năng quan trọng nhất của IDS => Giám sát+cảnh báo+bảo vệ\*
51. Ưu điểm NIDS(chọn 2)=>qly network segment+trong suốt vs ng dùng
52. Mô tả đúng vs HIDS (chọn 2)=>chỉ gsát hđ trên 1 máy tính+đặt trên các host xung tuyến of …DMZ
53. Mô tả ưu điểm của HIDS=>knăng xđ ng dùng lquan đến 1 sự kiện
54. Nhược điểm của HIDS => HIDS phải đk thiết lập trên từng host giám sát
55. Tường lửa cổng chuyển mạch đh theo quy tắc => ktra phiên kết nối
56. Tg lửa lọc gói tin ktra =>cổng nguồn và đích + IP nguồn đích of gói tin
57. Tg lửa cứng có đặc điểm =>là thiết bị tg lửa chuyên dụng
58. Tg lửa ko phải là thương mại => Iptables
59. Tg lửa ko lm đk => phát hiện mã độc + định danh
60. Tg lửa cá nhân ko lm đk =>ksoát luồng data cho 1 dải mạng

67. c năng IP SEC thiết lập sự bảo mật t/ứ giữa 2 đối tượng ngang hàng, xđ khóa, g thức, t.toán..=>Sai

(2)

1. Công nghệ chia 1 mạng bên trong thành mạng logic nhỏ, dễ sd hơn => VLAN
2. Ko sd 1 l.kết chuyên dụng, pp kết nối 2 mạng xa nhau an toàn =>VPN
3. Cố gắng đăng nhập máy tính 3 lần, khóa tài khoản=>HT phát hiện xâm nhập đã vô hiệu hóa TK user
4. Giải pháp giúp router hay switch điều khiển từ xa => danh sách đ khiển truy cập (ACL)
5. Phần nào của t bị cứng có thể dk nâng cấp bảo mật tốt=> phần sụn(firmware + tệp tin cấu hình)
6. G thức cần xóa trên router => ICMP
7. G thức cần xóa trên 1 máy chủ mail => SNMP
8. G pháp cần lm vs 1 mail server để ngăn user ngoài gửi mail thông qua nó=>hạn chế c tiếp tínhiệu SMTP
9. Đặc tính ko thuộc c năng bảo mật TT trog mật mã => hiệu quả
10. Hệ mật ng gửi,nhận sd cùng 1 khóa khi mã hóa vs giải mã =>đối xứng
11. Chuẩn mã Mỹ thay thế cho DES =>AES
12. Hệ mật ng gửi + nhận sd khóa khác nhau để mã hóa/giải mã=>bất đối xứng
13. Giao thức/thuật toán là nền tảng cơ sở hạ tầng khóa công khai(PKI)=>MD4
14. Gtrj hàm băm of 2 thông điệp khác nhau có giá trị tương tự nhau => xung đột
15. Thực thể cho phép phát hành , q lý, p phối các chứng thư số =>quyền cấp chứng chỉ
16. Pp sinh trắc học an toàn nhất =>vân tay
17. 1 ng gọi đến q lý báo mất mật khẩu => xác minh danh tính of họ trc khi cấp
18. Pp xác thực sd 1 KDC để xác thực =>kerberos
19. Pp xác thực gửi yc cho máy trạm và dk mã hóa gửi lại máy chủ => CHAP
20. G thức/d vụ cần loại bỏ trong mạng nếu có thể => ICMP
21. Kỹ thuật cho phép tạo k.nối ảo giữa 2 mạng sd 1 g thức bảo mật => tunelling
22. Cung cấp inf cho cty về tin tặc giúp ích nhiều nhất => các điểm yếu
23. Khi 1 ng dùng báo HT of a ta p hiện 1 virus mới =>ktra lại pm diệt virus hiện hành
24. Yếu tố hữu ích nhất trong việc k.soát tấn công từ ngoài => system logs
25. Cài 1 máy chủ cung cấp d vụ web đến máy trạm tránh rủi ro=>cài đặt máy chủ trong 1 DMZ
26. Loại tấn công dẫn đến việc truy cập of user hợp pháp đến các mạng bị từ chối =>DOS
27. Loại tấn công sd nhiều hơn 1 máy tính để tấn công nạn nhân =>DDOS
28. 1 máy chủ trên mạng có 1 ctr đang chạy quá thẩm quyền =>tấn công back door
29. Nỗ lực tấn công vào 1 phiên liên lạc = 1 máy tính giữa 2 HT => t.công ‘man in the middle’
30. Dạng tấn công sd 1 chứng chỉ đã hết hiệu lực đòi giành đăng nhập=>t.công TCP/IP hijacking
31. 1 máy chủ trên mạng chấp nhận các nối TCP =>t.công TCP ACK
32. Tấn công Smurf sd =>ICMP kết nối
33. Dạng virus đính kèm chính nó vào boot sector of đĩa cứng =>Stealth virus
34. 1 ctr đk ẩn vào 1 ctr khác đc cài vào HT => Trojan horse
35. User trog mạng nội bộ báo HT của họ bị nhiễm mã độcnhiều lần=>máy chủ cóthể là vật lây nhiễm virus
36. Các log file trên HT p.hiện 1 nỗ lực giành quyền truy cập =>tấn công đoán mật khẩu
37. 1 user báo a ta nhận 1 lỗi chỉ ra địa chỉ TCP/IP đã sd nhiều khi bật máy tính=>t.công TCP/IP hijacking
38. (giống câu 1 đề 1)
39. Bộ lọc gói tin thực hiện => ngăn chặn gói tin trái phép đi từ mạng bên ngoài
40. Yêu cầu cho VPN lớp 1(chọn 2)=> Mã hóa data dvao DES + qly key dựa vào IKE
41. Yêu cầu cho VPN lớp 2(chọn 2)=> Mã hóa data dựa vào IPSEC và 3DES + qly key dựa vào IKE
42. Yêu cầu cho VPN lớp 4=> Kết nối ISPvoiws 1 SLA + Dvụ tm tt như LDAP+ tốc độ truy cập cao ISDN và xDSL cùng T1 và T3.
43. Cơ chế xác thực ng dùng sd ở các điểm VPN muốn truy xuất => đăng nhập ID + password
44. Mã hóa data trog VPN giúp ngăn tấn công => xem data trái phép
45. Mô tả đúng vs pp p.hiện tấn công dựa trên dấu hiệu =>dế phát triển, cho phản hồi cxac về cảnh báo,yc ít tài nguyên tính toán
46. Mô hình mô phỏng cho HT IDS : Stateful IDS
47. HT có k.năng p.hiện xâm nhập, tấn công, tự động ngăn chặn là HT: IPS
48. Kiến trúc chung của IPS(chọn 3)=> Module ptich luồng data + p.hiện t.công + phản ứng.
49. Kiến trúc IPS bao gồm: IPS mạng trong/mạng ngoài
50. Các kỹ thuật p.hiện và ngăn chặn xâm nhập trog HT IPS : ABCD
51. Mô tả ưu điểm của honey port(chọn 3): thu nhập 1 vài inf chi tiết+công nghệ đơn giản+ tốt trog IPV6
52. Honey port đk chia lm các loại chính sau: tương tác thấp+tương tác cao
53. Honey wall sd các công cụ: IDS Snort+firewall iptables
54. Tường lửa ko thương mại=> iptables
55. Tg lửa ko lm đk => phát hiện mã độc + định danh ng dùng
56. Tg lửa cá nhân ko lm đk: k.soát data cho 1 dải mạng
57. Tg lửa mềm: Microsoft ISA 2006
58. Chuẩn 802.11a đúng => 802.11a và 802.11b ko tương thích
59. Mạng vô tuyến đô thị WMAN sd chuẩn => 802.16
60. Trog mạng ko dây sd BSSID => tên địa chỉ MAC
61. Tg lửa phát hiện đk mã độc => sai
62. Tg lửa ko bảo vệ mạng tin cậy => sai



81. Lệnh truy cập SSH tại máy chủ mạng DMZ => iptables -A INPUT -p tcp --dport 22 -j ACCEPT

82.Lệnh cho phép trang mạng LAN t.cập SSH tới máy chủ ngoài Internet=> iptables -A OUTPUT -o eth0 -p tcp -dport22 -m state --state NEW,ESTABLISHED -j ACCEPT

83.Lệnh cho phép ngdung Internet truy cập tới máy chủ web trong DMZ => iptable -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.2.2.10:80

84.Lệnh cho phép ngdung Internet gửi nhận mail tới DMZ => iptables -t nat -A POSTROUTING -i eth0 -p tcp -m multiport --dports 25,110,143 -j SNAT -- to-destination 10.2.2.10

85.Lệnh cho phép ngdung LAN gửi nhận mail ngoài Internet => iptables -t nat -A POSTROUTING -o eth0 -p tcp -m multiport --dport25,110,143 -m state --state NEW,ESTABLISHED -j ACCEPT

86.Lệnh chặn Hacker vs IP đã cho kết nối trong DMZ => iptables -A INPUT -i eth0 -p tcp -s “192.168.114.10” -m state --state NEW,ESTABLISHED –j DROP

87. Lệnh cho phép máy tính bên trong truy vấn DNS bên ngoài=> iptables -A OUTPUT -p udp -o eth0 –dport 53 -j ACCEPT

88. Luật cho Snort p.hiện t.công Ping Of Daeth?=>alert tcp any any -> any any(msg:”ICMP Ping Of Death”;itype:8;dsize:>1000;detection\_filter:track by\_src, count 1000, seconds 10; classtype:denial-of-service;sid:2100222;rev:2;)

89. Luật cho Snort p.hiện t.công SCAN?=> alert tcp any any -> any any(msg:”SYN FIN scan attack”; detection\_filter:track by\_src, count 1000, seconds 5; flags:S; classtype:network-scan; sid:200384; rev:2;)

90. Luật cho Snort p.hiện t.công mk? => alert tcp any any -> $HOME\_NET 21 (msg:”FTP Brute force Attack”; flow:from\_server, established; content:”530”; pcre:”/^530\s+(Login|User)/smi”; classtype:unsuccessful-user;threshold:type threshold, track by\_dst,count 5, seconds 60; sid:2002383; rev:3;)

(3)

1. G thức lm việc trên lớp IP để bảo vệ TT IP trên mạng => IPSEC
2. LAC và LNS là tp of g thức đg hầm =>L2TP
3. Mã khóa công khai là: 1 khóa mã-1 khóa giải+ có thể dùng khóa public mã hóa
4. G thức sd rộng rãi nhất để truy cập kiểu quay số đến 1 máy chủ từ xa => SLIP + PPP
5. Ký thuật sd truyền data qua mạng ko đc bảo mật =>VPN
6. Chuẩn g.thức mạng ko dây pp nd (WML) đến (PDA) =>WAP
7. Chứng thư số chứa inf => chữ kí + thuật toán tạo mã khóa +tạo chữ ký
8. Nên cài mức truy cập mặc định => NO access
9. Quyền truy cập cho phép hiệu chỉnh thuộc tính of 1 tệp tin =>Modify
10. C sách tài khoản nên đk thiết lập ngăn các cuộc t.công vào TK ng dùng=>g.hạn số lần đăng nhập
11. Chiều dài tối thiểu của 1 mật khẩu mạnh =>8 ký tự
12. Tấn công Flood từ các máy đến 1 webserver => DDOS + tấn công IP
13. Để ngăn t.công DoS,1 q.trị mạng chặn IP vs tường lửa,t.công vẫn tiếp. Khả năng xảy ra?=>Sâu DoS lây nhiễm cục bộ+pm Antivirus cần cđ trên máy chủ đích.
14. Loại khóa mật mã dễ bị tấn công nhất => 40 bít
15. Cách tốt nhất để chống lại điểm yếu bảo mật trog HĐH => cài bản server pack mới nhất
16. mk khó phá nhất đối vs hacker => !$aLtNb83
17. Kỹ thuật s.dụng bảo đảm tt liên lạc qua 1 mạng ko bảo mật => Telnet
18. Các chuẩn giao thức mạng pp ND Wireless Markup Language (WML) đến ỨD Web trên t.bi cầm tay (PDA)? => WAP
19. Các chuẩn g.thức mạng ko dây IEEE phổ biến nhất => 802.11.b/a/g
20. Mức mã hóa WEP nên đc thiết lập trên 1 mạng 802.11b =>128 bít
21. Cơ cấu bảo mật ko dây ít an toàn nhất => bảo mật sd định danh mạng
22. Bộ lọc địa chỉ MAC định ngĩa như=> tg lửa cá x+ngăn chặn/truy cập đến 1 MAC nhất định
23. Pp điều khiển truy cập có hiệu quả an toàn nhất đvs mạng ko dây =>nhận dạng bảo mật mạng
24. Cơ chế bảo mật đc sd vs chuẩn ko dây WAP => WTLS
25. Thiết bị sd bộ lọc gói + quy tắc truy cập => tường lửa
26. T bị cho phép kết nối đến 1 mạng LAN qua 1 kênh dk mã hóa an toàn => máy chủ VPN
27. ứng dụng để ptich + ktra lưu lượng mạng => Sniffer
28. cần lm j để bảo vệ data trên máy tính xách tay => mã hóa data
29. ngăn chặn ghi đè data trên tbj lưu trữ => t lập tab “ wirte protect”
30. phương tiện ko bị ảnh hưởng bởi từ tính => băng từ
31. yếu tố cần sd tích hợp vs 1 thẻ thông minh để xác thực =>mã pin
32. t bị lưu trữ ko cơ động đc => ổ đĩa cd
33. t bị để theo dõi cảnh báo tới quản trị mạng => HT phát hiện xâm nhập (IDS)
34. phân vùng mạng chứa các máy chủ internet => DMZ
35. loại mạng mô tả cho ctr bên trong cho mô hình B2B => intranet
36. Dvu mạng cho phép các địa chỉ mạng bên trog dc che giấu => NAT
37. ?
38. IPSEC cung cấp sự mã hóa data + xác thực of 1 t.lập VPN => client tới server
39. Trong mối qhe tin cậy 2 chiều, tin tặc **ko** thể thực hiện trực tiếp trong VPN.
40. VPN trực tiếp có thể dựa trên nd of các gói data để điều khiển truy cập => có
41. Dựa trên lớp l.kết, VPN lớp l.kết chia thành => 3 loại(PPTP,L2F,L2TP)
42. VPN lớp mạng tổ chức theo=> mô hình VPN ngang hàng + che phủ
43. VPN có thể chia thành => 5 lớp (0->4)
44. Những ưu điểm của HT HIDS => có k.năng xđ ng dùng liên quan tới 1 sự kiện
45. Những nhược điểm của HT HIDS => HIDS phải đk thiết lập trên từng host cần giám sát
46. Những mô tả đúng vs pp p.hiện t.công dựa trên dấu hiệu=> giống câu 45-đề 2( chọn cả 3 đáp án)
47. HT có k.năng p.hiện sự xâm nhập, t.công, ngăn chặn các cuộc t.công là => HT IPS
48. Kiến trúc chung of HT IPS(chọn 3)=>module p.tích luồng data+p.hiện t.công+phản ứng
49. Kiến trúc IPS gồm=>IPS mạng trong+mạng ngoài
50. Các ký thuật p.hiện và ngăn chặn xâm nhập áp dụng trong HT IPS=> chọn tất cả
51. Tường lửa ko lm đk => p.hiện mã độc+ định danh ng dùng
52. Tg lửa cá X ko lm đk => k.soát luồng data cho 1 dải mạng
53. Tg lửa mềm => microsoft ISA 2006
54. Loại t.công đc đ.nghĩa là truy cập TT ko x.thực từ t.bị ko dây thông qua bluetooth => Bluesnarfing
55. Pp p.hiện hiệu quả nhất dạng t.công giả mạo AP=>cài đặt HT p.hiện xâm nhập mạng ko dây
56. Nhiều khi t.công từ chối DOS, mạng ko dây tại nhà vấn đề k.nối ko liên tục chiều, tối=> ai đó đang t.công từ chối dvu vào mạng với VOID 11
57. Bob lo lắng về AT mạng ko dây, vô hiệu hóa SSID, Bob k.định mạng ko thể bị t.công => Ngay cả khi SSID bị tắt vẫn có thể nghe lén mạng
58. Ưu điểm of Honeypot (chọn 3)=> thu thập 1 vài inf chi tiết+công nghệ đơn giản+tốt trong IPV6
59. Honeypot chia lm các loại chính(chọn 2)=> tương tác thấp+ tương tác cao

68. c năng IPSEC thiết lập bảo mật giữa 2 đối tượng ngang hàng,xđ khóa, thuật toán, giao thức=> sai

70. đg hầm kĩ thuật đóng gói toàn bộ data bất kì of các giao thức. Phần header... đến điểm đich => sai

71. lớp trog mô hình OSI là đích of hầu hết t.công mạng cơ bản=> lớp ứng dụng

72. thuật ngữ “drive-by-dowload”=>truy cập trang web có mã độc tự động thực thi ko cần kích hoạt

73. thẩm định đầu vào thích hợp of data truyền nên bao gồm=>loại dữ liệu

74. nhiều user dùng máy tính đã bị xâm nhập do khai thác lỗ hổng of java...=>cài bản vá ms nhất.., sd IE..

75. bạn đc giao đ.giá rủi ro 1 ứng dụng ở cty.ai nên kết hợp=> các t.viên đội bảo mật,...hđ của ứng dụng

76.bạn đ.giá AT cho máy chủ web cty x.định lỗ hổng cross-site scripting =>khuyên q.trị web đ.bảo data input

77. bạn ms triển khai bộ cs AT cho user of tổ chức=> giới hạn máy trạm P2P

78. ko phải là 1 pha trog x.lý mh đ.giá rủi ro=> định nghĩa các đối tượng an toàn

79. Bob cbj đ.giá AT trên windows XP, lo lắng buffer overflows => cài đặt bản vá ms nhất

80. bạn ms cài đặt CSDL SQL bên trong mạng nội bộ, triển khai loại hình IDS=>dựa trên host đc t.khai trên máy chủ SQL

(4)

21. mạng riêng ảo VPN sd g.pháp AT =>tunneling+mã hóa+xác thực+ủy quyền

22. giao thức sd trong VPN=> IPSEC+PPTP+L2TP

23. những mô tả là ưu điểm của VPN => chí phí triển khai thấp+ tính bảo mật cao

24. mạng riêng ảo VPN đc p.loại thành nhóm=>remote access VPN + intranet VPN + extranet VPN

25. mạng intranet VPN đc sd để k.nối=>các văn phòng chi nhánh of tổ chức vs mạng intranet trung tâm

26. ưu điểm of intranet VPN=>dễ dàng thiết lập các kết nối peer-to-peer mới

27. ưu điểm chính of extranet VPN => giảm chi phí nhiều so vs pp truyền thống

28. nhược điểm of extranet VPN => khó khăn cài đặt, bảo trì và chỉnh sửa t.lập có sẵn

29. c.năng chính of VPN server =>lắng nghe các yc kết nối+dàn xếp các yc và thông số k.nối+xác thực ..VPN

30. mô tả là tiêu biểu of 1 VPN client=>các g.tiếp từ xa sd internet or mạng công khai kết nối of tổ chức từ nhà

31. HT p.hiện t.công bắt giữ gói tin trên tbj mạng(hữu+vô tuyến) so2 vs CSDL mẫu p.hiện t.công=>network IDS hoặc NIDS.

32. HT p.hiện xâm nhập đc cài đặt như tác x máy chủ, xem tệp tin log of các trình ứng dụng =>host IDS or HIDS

33. tbj bảo mật ko phải IDS=> chọn tất cả

34. c.năng quan trọng nhất của IDS =>cảnh báo

35. ưu điểm of NIDS(chọn 2)=>q.lý cả 1 network segment+trong suốt vs ng dùng lẫn kẻ tấn công

36. mô tả đúng vs HT HIDS(chọn 2)=>chỉ g.sát các hđ trên 1 máy tính+ thường đặt trên host xung tuyến..DMZ

37. ưu điểm of honeypot(chọn 3)=>thu thập inf chi tiết+công nghệ đơn giản+lm tốt trong IPV6

38. kiểm soát luồng data, chặn tin tặc , Honeywall sd công cụ=> IDS Snort + Firewall iptables

39. mô hình dưới đây mô tả cấu trúc lm việc của => Snort\_inline

40. mô hình Honeynet là thế hệ => thế hệ I

41. iptables cung cấp tính năng => chọn tất cả

42. v. Trò tường lửa => điều khiển lưu lượng mạng

43. p.loại tường lửa theo c.năng=>lọc gói tin + cổng chuyển mạch + ứng dụng

44. tg lửa ứng dụng hđ ntn=>ktra g.thức tần ứng dụng of gói tin

45. tg lửa hđtại những tầng OSI => tầng 3,4,5,7

46. tg lửa cổng chuyển mạch hđ theo quy tắc => ktra phiên kết nối

47. tg lửa lọc gói ktra TT gì of gói tin=> cổng nguồn và đích + địa chỉ IP nguồn đích

48. tg lửa cứng => là tbj tg lửa chuyên dụng

49. tg lửa ko phải thương mại => Iptables

50. tg lửa ko lm đc=>phát hiện mã độc + định danh ng dùng

51. giao thức bảo mật WEP sd chuẩn mã => RC4

52. pương tiện TT liên lạc trong mạng ko dây => access point

53. tbi ko dây truyền thông trực tiếp qua nhau ko qua AP => ad-hoc mode

54. lớp ko hợp lệ của bluetooth => Class 0

55. tại sao tiến hành khảo sát vtri cty=> ghi lại các t.hiệu mạn ko dây và gợi ý nâng cấp

56. công cụ NetStumbler dùng để =>khảo sát mạng

57. TEMPEST là định nghĩa cho =>1 công cụ nghe lén bị động

58. gửi thông điệp ko đc yc qua bluetooth=> Bluejacking

59. Bob lo lắng an toàn mạng ko dây, vô hiệu hóa SSID => ngay cả khi SSID bị tắt vẫn có thể nghe lén mạng

60. phát biểu sai WPA2=> sử dụng hệ mật RSA

64. T.toán Diff-hellman, mỗi thực thể g.tiếp cần 2 khóa, 1 để phân phối, 1 là khóa riêng=> sai