Övningstentamen Linux Network Security

Linuxsystem ls10, Nackademin YH 2011

Ett poäng för varje rätt besvarad fråga, inga halva poäng. G=20 VG=32

Inga hjälpmedel vid sidan av penna och suddgummi ***Lycka Till!***

Namn: ….....

Privat epost: ….....

Telefon: ….....

1. Vad är en studsattack mot ftp? (ftp bounce attack?)

   a. angriparen kan inte komma in eftersom tjänsten är så säker

   b. användaren skickar listiga kommandon, som gör att en ftp-tjänst kan användas för att skicka trafik vidare till det system som är målet för angreppet

   c. användaren försöker ladda upp för stora filer som inte får plats och när detta inte går, kallas det att filen studsar på ftp-tjänsten

   d. det är när ftp-servern nått sitt kapacitetstak så att inga ytterligare användare kan tillåtas att komma in i systemet

2. Vad gäller för själva ftp-protokollet?

   a. det är enkelt och rättframt och ställer sällan till problem

   b. det är väldigt säkert eftersom det går att skydda med lösenord och liknande

   c. det använder samma socket för kommandon och dataflöde

   d. det använder olika socket för kommando och dataflöde

3. Vad är en buffer overflow och varför vill du inte ha sådana?

   a. det är när angriparen matar in mer data än vad programmet förväntat sej så att själva programkoden skrivs över med det som matats in

   b. det är när en switch lastats ner med så tung trafik att dess mac-tabell inte räcker

   c. det är den teknik som används för att omvandla vattenkraft till elenergi

   d. angriparen får möjlighet att köra egna program på din maskin

4. Varför räcker inte en effektiv brandvägg för att stoppa intrång i ditt nätverk?

   a. netfilter överbelastas om trafiken är för tung och då släpps all trafik igenom

   b. dina användare gör dumma saker med både webbläsare och minnepinnar

   c. angriparen kan många gånger skada dina system redan genom de portar du redan håller öppna

   d. om dina certifikat är defekta fungerar inte brandväggen tillfredställande

5. Vad kan du använda för att sätta upp en ssh-tjänst på ett säkert sätt?

   a. förutdelade nycklar
   b. ställa in så att root inte får logga in direkt
   c. sunt förnuft
   d. /etc/hosts.allow och /etc/hosts.deny

6. Varför kan UDP-baserad kommunikation vara ett säkerhetsproblem?

   a. det är svårt att avgöra om ett givet paket tillhör något etablerat dataflöde

   b. UDP tillåter inte kryptering vilket är ett mycket stor problem

   c. med UDP måste hastigheten hela tiden ökas vilket försvårar för kommunikationsprogram

   d. användaren tillåts inte autenticera sej med UDP-baserad kommunikation

7. Din chef säger att du måste säkra upp nätverket bättre fastän du installerat och konfigurerat moderna switchar, vilka problem tror du hon tänker på när det gäller just switcharna?

   a. begränsa antalet mac-adresser per port, så blir det svårt att flöda över mac-tabellen

   b. begränsa antalet mac-datorer på nätet så att dessa inte förstör säkerhetsarbetet

   c. se till att låsa vlan-konfiguration så att användarna inte själv kan hoppa mellan olika vlan

   d. switcharna låses så att de inte går att administrera via telnet

8. När chefen ändå är igång nämner hon även risken för en smurf-attack, vad är det?

   a. det har i alla fall inget att göra med nätverkssäkerhet...

   b. genom att skicka ping på broadcast-adressen så kan ett helt nät fås att svara på pinget, som då riktas mot tredje part

   c. genom att skicka listiga paket på en brandvägg så kan den förmås att koppla upp en session till varje enhet på nätverket bakom ”väggen”

   d. en brandvägg har normalt tre anslutningar, grön: lokalt nät, röd: internet och blå: dmz, det nät där maskiner som skall vara tillgänglig för alla kopplas; vid en smurfattack angriper man de senare datorerna med en kombination av brute force och DOS

9. Vilka säkerhetsproblem kan en DNS-tjänst ha?

   a. normalt sett inga om man behärskar Bind

   b. rent historiskt har programmet Bind haft många säkerhetsluckor

   c. dns-tjänsten sprider information om maskiner som (normal) inte är tillgängliga

   d. zonöverföring tillåts urskiljningslöst (utan några regler eller hinder)

10. Hur motverkar du säkerhetsproblem i din DNS?

    a. uppdaterar Bind vart efter det kommer olika patchar

    b. använd ACL:er för att styra användningen

    c. konfigurera med flera vyer

    d. tillåt inte zonöverföring med andra maskiner än dina egna

11. Din näsvisa chef vill att du använder TSIG, men till vad?

    a. Termination Security Interface Group gör säkra nätverksadaptrar som är dyra och bra

    b. Trusted Security Initiative Group rapporterar om aktuella säkerhetsproblem

    c. Traditional Security Information Group informerar om säkra lösenord och hantering av id

    d. Transaction SIGnature signerar zonöverföringar och andra DNS-operationer

12. För att göra henne nöjd passar du även på att skärpa till företagets brandvägg, men hon verkar ändå bekymrad över säkerheten därför att...

    a. hon inte litar på att du behärskar iptables

    b. en brandvägg kan inte hindra ett intrång via http (port 80)

    c. användarna surfar själv hem fulkod

    d. de tjänster som släpps igenom kan även användas som angreppsväg

13. När du ändå är igång installerar du även intrångsdetektering med hjälp av snort, men...

    a. snort genererar fantastiska mängder loggar som gör dej helt förvirrad

    b. du hittar inga aktuella regler att tanka hem

    c. trafikmängden i ditt nätverk gör att snort lastar ner datorn för mycket när du kör snort

    d. snort ger bara falska larm om trafiken är krypterad

14. Så du tittar på företagets webbserver som kör Wordpress med hjälp av (bland annat) Apache och MySQL och därför bör du:

    a. se till att all PHP-kod skrivs om

    b. skydda de tjänster som inte skall vara tillgängliga utifrån

    c. se till att alla delkomponenter, även databasen, har en säker konfiguration

    d. övertyga chefen om att gå över till Joomla

15. För att se hur de lokala brandväggsreglerna på webb-servermaskinen använder du kommandot:

    a. iptables --show

    b. iptables --display

    c. iptables –L

    d. iptables –l

16. Eftersom reglerna var en röra vill du radera dem och börja på ny kula med hjälp av:

    a. iptables --reconfigure-all

    b. iptables --delete-all

    c. iptables -D

    d. iptables -F

17. Du börjar känna dej varm i kläderna med iptables, vad är fördelarna med att skriva sina regler själv?

    a. man är säker på att det alltid blir rätt

    b. en människa kan oftast skriva enklare regler som utnyttjar maskinen effektivare

    c. verktyg för regelhantering är oftast mycket svåra att använda

    d. maskingenererade regler innehåller oftast säkerhetsluckor

18. Varför kan det trots detta ändå vara bättre att ta hjälp av ett verktyg för att ordna brandväggsreglerna?

    a. det är oftast enklare med verktyg om brandväggens specifikation är någorlunda komplex

    b. trots en komplex väv av iptables-kommandon så gör verktyg hanteringen säker

    c. moderna verktyg gör brandväggen snabbare än manuellt gjorda, med iptables direkt

    d. verktyget i sig skapar ytterligare ett hinder som angriparen måste ta sig förbi

19. När du använder moderna protokoll med inbyggd kryptoteknik finns det trots detta vissa punkter som är känsligare för angrepp än andra:

    a. nyckelutbytet

    b. själva krypteringen

    c. nätverkets fördröjning (latens, latency)

    d. begränsningar i processorn

20. PKI (Publik Key Infrastrukture) låter toppen, men var finns svagheterna i tekniken?

    a. kopplingen mellan certifikatet och dess innehavare är oftast lösare än man vill tro

    b. den centrala CA-organisation som var ursprungstanken finns inte

    c. en lång rad CA-tjänster ha kompromenterats på sistone

    d. revokeringslistor används sällan fastän de egentligen är mycket viktiga

21. Vad är en revokeringslista?

    a. en lista över certifikat som inte längre är pålitliga

    b. en lista över ca-tjänster som inte längre är pålitliga

    c. en lista över maskiner som skrotats

    d. en lista över olämpliga kryptonycklar

22. Eftersom du använder HTTPS när du loggar på i din favoritkommunity på webben så borde du vara helt säker, eller?!

    a. med hjälp av en kompromenterad ca-tjänst skaffas enkelt certifikat som lurar användaren

    b. det finns flera kända så kallade man in the middle attacker mot HTTPS

    c. HTTPS behöver inte alltid betyda att det verkligen används krypterad kommunikation

    d. alla populära webbtjänster som hanterar personlig information prioriterar användarna integritet och säkerhet framför allt annat

23. Vad innebär en arp-förgiftning?

    a. det betyder att företagets router utsatts för en denial of service och därför fungerar dåligt

    b. webbserverns certifikat har bytts ut mot falska certifikat av okänt ursprung

    c. med hjälp av ARP förmås maskinerna på ett nätverk att byta default gateway

    d. att du skall sjukskriva dej minst en vecka

24. Du börjar känna dej trött på alla osäkerheter du stött på och vill därför börja använda ssh för att:

    a. säkra terminalsessioner över nätet

    b. kryptera eposten

    c. användarna skall kunna verifiera att de anslutit sig mot rätt maskin

    d. skapa krypterade länkar mellan olika nät

25. För att ytterligare öka säkerheten med ssh vill du:

    a. förhindra rootinloggning

    b. kräva att användarna autenticerar sej med S/KEY

    c. dela nycklar mellan server och klienter på förhand

    d. förhindra åtkomst med gamla protokollvarianter

26. Varför kan det vara svårt att använda nycklar som delats i förväg i en större organisation?

    a. alla steg som måste göras på en maskin och med en användare multipliceras med antalet maskiner och användare så blir det snart stora tal

    b. facket motarbetar ofta användningen av modern kryptoteknik eftersom de är rädda om sina medlemmars integritet

    c. bolagets styrelse måste alltid informeras och detta tar ofta både tid och resurser

    d. mängden nycklar minskar drastiskt säkerhetsnivån i företagets nätverk

27. Du skall skicka epost till din kollega i USA och funderar över säkerheten:

    a. USA är en vänligt sinnad nation så det är förmodligen ingenting att oroa sej över

    b. jag använder TLS och bra autenticering när jag skicka eposten så då kan det inte bli fel

    c. epost skickas -nästan- alltid i klartext mellan två epostservrar

    d. det kan vara lämpligt att sätta upp en vpn-förbindelse till kollegan i USA

28. Du har blivit säkerhetsansvarig på ett företag, varför vill du inte att personalen skall kryptera sin epost?

    a. vi använder modern kryptoteknik (TLS över VPN-länk) när användarna kopplar upp sej

    b. om en anställd slutar så går det inte att läsa dennes epost utan aktiva hjälp från personen i fråga

    c. med moderna brandväggar behövs inga ytterligare säkerhetsåtgärder

    d. epost används ändå aldrig för någon verksamhetskritisk information

29. Vad är en DOS-attack?

    a. Disk Operating System, en enkel föregångare till Windows och OS/2

    b. Distributed Outbound Scan, en avancerad portskanningsmetod som inte kna upptäckas

    c. Denial Of Software, angriparen förhindrar offret att använda mjukvara

    d. Denial Of Service, angriparen orsakar så hög belastning att användaren inte kommer åt sina resurser

30. Varför vill din chef centralisera logghanteringen på era system?

    a. han vill flytta allt till huvudkontoret i Dubai

    b. för att göra det svårare för angriparen att sudda ut spåren

    c. för att göra det enklare för administratören att se vad som händer på maskinerna

    d. för att vara säker på att svagheter i ssh:s nyckelutbyte inte orsakar sämre loggning

31. När du tittar i loggarna verkar det som om din nätverksskrivare försöker portskanna din DNS-maskin...

    a. det är säkert något fel, för en gammal LaserJet kan ju inte portskanna...

    b. angriparen arp-spoofar ditt nät och du blir tvungen att söka ett nytt jobb

    c. din skrivare är förmodligen utsatt för en så kallad ftp-bounce

    d. skivaren måste startas om och du får ladda toner inan du kan släppa ut den på nätet igen

32. /etc/host.deny gör att du enkelt kan:

    a. bestämma vilka maskiner som släpps in

    b. du kan minska belastningen nätverket utan att skapa några andra problem

    c. med rsynk kan enkelt host.deny hållas fräsch

    d. det går inte att blockera ftp med hosts.deny

33. Kan xinetd...

    a. skapa ytterligare säkerhet kring tjänster utan säkerhetsannordningar

    b. kan köra dina skript som du enkelt kan få att bli moderna nättjänster, med hjälp av xinetd

    c. xinetd kan logga sina aktiviteter utförligt

    d. xinetd fungerar inte på system där anacron är aktivt

34. Eftersom du har är duktig på iptables tycker du att det verkar onödigt att köra chroot till dina tjänster, men...

    a. chroot förhindrar program att komma åt information utanför sin chroot-miljö

    b. chroot är ett enkelt sätt att öka säkerheten på många typer av tjänster

    c. iptables och chroot löser helt olika problem

    d. chroot fungerar inte i användarnas hemkataloger

35. Du skall koppla in en dator för ordermottagning, som sitter på det publika nätet i företagets foaje. Vad kan du göra för att skärpa upp säkerheten trots den olämpliga placeringen av datorn?

    a. ssh-tunnel

    b. /etc/hosts.allow och /etc/hosts.deny

    c. iptables

    d. genom att köra nmap på alla datorer i foajen

36. Vad är en drive-by attack?

    a. någon bryter sej in på nätverket via wifi från parkeringen

    b. någon kopplar in sej på en RJ-45:a i receptionen

    c. användarna luras att köra fulprogram i sina webbläsare när de besöker en webbplats

    d. en hacker bryter sej in i företagets lokaler för att stjäla information

37. Vad gör en honungsfälla (honey-pot)?

    a. det är något med biodling och har inte med it-säkerhet att göra

    b. man sätter upp en maskin som verkar innehålla intressanta saker som håller angriparna sysselsatta

    c. brandväggen skickar angriparna vidare till någon annans nätverk

    d. iptables konfigureras så att alting verkar fungera men det går väldigt långsamt

38. Din chef har sett att din DNS-server går att komma åt både via TCP och UDP och därför måste du:

    a. blockera UDP eftersom det finns säkerhetsbrister i det protokollet

    b. blockera TCP för att det är ineffektivt

    c. göra ingenting för det är precis så det skall vara

    d. TSIG fungerar inte över TCP

39. Med fragmenterade paket så...

    a. kan det vara svårt att bedömma om trafiken är legitim

    b. så ökar nätets prestanda med 38%

    c. minskar hastigheten samtidigt som säkerheten ökar för windowsklienter

    d. händer ingenting speciellt eftersom detta är helt enligt RFC-2097

40. Eftersom du är tvungen att använda telnet så...

    a. skickas dina lösenord i klartext

    b. skickas all trafik i klartext

    c. krypteras eposten enklast med gpg

    d. kan du lura inkräktarna att ni är ett gäng klåpare som de kan äga utan att anstränga sig

Rätta svar:

1. b	2. d	3. ad	4. bc	5. abcd	6. a
7. ac(d)	8. b	9. bcd	10. abcd	11. d	12. (a)cd
13. a(b)c	14. bc	15. c	16. d		

17. b (och ibland c för man kan få spader av vissa verktyg...)

18. ab	19. a	20. a(bc)d	21. a	22. abc	23. c
24. acd	25. abcd	26. a	27. c(d)	28. b	29. d
30. (a)bc	31. c	32. a	33. abc	34. abc	35. abc
36. c	37. b	38. c	39. a	40. ab(d)	