DIGINTO
Tenta 2019

PROV i Nätverkssäkerhet

1.

Vilket skadligt program kan inte göra någonting förrän åtgärder vidtas för aktivering av det bifogat skadligt programmet?

2.

Cookies är små informationsobjekt (textfiler) som lagras på användarnas datorer och används i stor utsträckning av onlinetjänstleverantörer för flera ändamål, till exempel för att fånga användarinställningar (språk, bakgrundsfärger, etc.), för att identifiera användaren när han/hon använder en inköpslista etc. På så sätt har kakor verkligen positiva funktioner (t.ex. hjälper de till att undvika behovet av att upprepade gånger behöva identifiera sig).

Men cookies väcker också vissa säkerhets- och integritetsproblem, kan du ge någon exempel?

3.

Ganska ofta behöver du använda öppna Wi-Fi-nätverk, t.ex. på tågstationer eller kaféer. Du är dock medveten om att det kan finnas faror med sådana öppna nätverk. Vad kan du göra för att skydda din kommunikation över dessa offentliga nätverk?

4.

Vilka nätverkssäkerhetslösningar kan användas för att mildra DoS-attacker?

5.

Vad kännetecknar DoS -attacker?

6.

En hacker använder en bärbar dator som en open åtkomstpunkt för att fånga all nätverkstrafik från en utvald användare. Vilken typ av attack är detta?

7.

Vad påverkar ett företag när det gäller ett säkerhetspolicy?

8.

Vad är den primära metoden för att mildra skadligt programvara?

9.

Vad kännetecknar en trojansk häst när det gäller nätverkssäkerhet?

10.

Hur konfigureras SSH version 2?

11.

Hur konfigureras en TACACS+ server?

12.

Hur konfigureras en RADIUS server?

13.

Vilka kommando krävs för att skapa ett användarnamn för admin, hasha lösenordet med MD5 och använda den lokala databasen för inloggning?

14.

Hur skapas olika användarkonto med olika behörigheter?

15.

Vad är standardbehörighetsnivån för användarkonton som skapas på Cisco-routrar?

16.

Vad för funktion har en RADIUS server?

17.

På grund av implementerade säkerhetskontroller kan en användare bara komma åt en server med FTP. Vilken AAA -komponent uppnår detta?

18.

Vilket inkommande ICMP-meddelande bör tillåtas på ett outside interface för att underlätta felsökningen?

19.

Vad innebär kommando nedan?

access-list 100 permit ip host 192.168.10.1 any

20.

Vad är CAM table overflow för något?

21.

Vilken CIA-princip åstadkoms med datakryptering?

22.

Hur kan DHCP-spoofing attacker mildras?

23.

Vilken typ av ACL erbjuder större flexibilitet och kontroll över nätverkstrafik?

24.

Vilka två protokoll används av AAA för att autentisera användare mot en central databas med användarnamn och lösenord?

25.

Vad är resultatet av att säkra Cisco IOS-image med funktionen Cisco IOS Resilient konfiguration?

26.

Vilka är informationssäkerhetens främsta mål?

27.

I vilka tillfällen kan en nätverksadministratör konfigurera åtkomstlistor på en router?

28.

Vilken wildcard mask är associerad med ett nätmask på /27?

29.

Definiera vad en spyware, ransomware, trojan, worm och virus.

30.

Blockera i 6 minuter åtkomst till router R1 efter 4 misslyckade inloggningsförsök som gjorts inom en tidsperiod på 2 minut.

31.

Efter hur många minuters inaktivitet kommer IOS att koppla bort en användare från konsolen eller VTY som default?

32.

Hur kan konfigureras en router för att stänga en session efter en 180 sekunder av inaktivitet?

33.

Marwan har installerat och konfigurerat sitt trådlösa nätverk. Han har aktiverat många säkerhetsfunktioner som att ändra standard-SSID, aktivera WPA-kryptering och aktivera MAC-filtrering på sin trådlösa router. Erik märker att när han använder sin trådlösa anslutning är hastigheten ibland 16 Mbps och ibland bara 8 Mbps eller mindre. Erik ansluter till routers hanteringsverktyg och får reda på att en maskin med ett okänt namn är ansluten via sin trådlösa anslutning. Erik kontrollerar routerns loggar och märker att den okända maskinen har samma MAC-adress som sin bärbara dator. Vilken av följande attacker har inträffat på Eriks trådlösa nätverk?