Iniciado em	domingo, 4 jun 2023, 16:32
Estado	Finalizada
Concluída em	domingo, 4 jun 2023, 16:37
Tempo empregado	5 minutos 37 segundos
Notas	12,33/13,00
Avaliar	**9,49** de um máximo de 10,00(**94,87**%)

Questão **1**

Correto

Atingiu 1,00 de 1,00

É ou são exemplos de NIDS:

- a. Suricata ✔
- b. OSSEC ✖
- c. Snort ✔
- d. AIDE ✖

Sua resposta está correta.

As respostas corretas são:
Snort,

Suricata

Questão **2**

Parcialmente correto

Atingiu 0,33 de 1,00

O que os NIDS normalmente não conseguem monitorar?

- a. Registros de log.
- b. Sistema de arquivos.
- c. Pacotes de redes.
- d. Processos do sistema. ✔

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.
As respostas corretas são:
Sistema de arquivos.,

Registros de log.,

Processos do sistema.

Questão **3**

Correto

Atingiu 1,00 de 1,00

Falso positivo ✔ é quando o IDS gera um alerta que não deveria, ou seja, classifica uma atividade normal como sendo um ataque.

Sua resposta está correta.

A resposta correta é:
[Falso positivo] é quando o IDS gera um alerta que não deveria, ou seja, classifica uma atividade normal como sendo um ataque.

Questão **4**

Correto

Atingiu 1,00 de 1,00

É ou são características de IDS baseado em comportamento:

- a. As anomalias são consideradas ataques. ✔
- b. Pode produzir mais falsos positivos do que o baseado em assinatura. ✔
- c. Mais complicado de configurar em relação ao baseado à assinatura. ✔
- d. Capaz de identificar ataques novos ou desconhecidos. ✔

Sua resposta está correta.

As respostas corretas são:
Mais complicado de configurar em relação ao baseado à assinatura.,

Capaz de identificar ataques novos ou desconhecidos.,

Pode produzir mais falsos positivos do que o baseado em assinatura., As anomalias são consideradas ataques.

Questão **5**

Correto

Atingiu 1,00 de 1,00

O que os HIDS podem monitorar?

- a. Sistema de arquivos. ✔
- b. Registros de log. ✔
- c. Pacotes de redes.
- d. Processos do sistema. ✔

Sua resposta está correta.

As respostas corretas são:
Sistema de arquivos.,

Registros de log.,

Processos do sistema.

Questão **6**

Correto

Atingiu 1,00 de 1,00

Qual ou quais dessas técnicas são conhecidas por identificar e reagir contra possíveis problemas de segurança?

- a. IPS ✔
- b. IDPS ✔
- c. IDS ✖
- d. AIDE

Sua resposta está correta.

As respostas corretas são:
IPS,

IDPS

Questão **7**

Correto

Atingiu 1,00 de 1,00

IDSs baseados em redes podem apresentar problemas em ambientes de rede que utilizam switches ou apresentam grande parte do seu fluxo de pacotes criptografado.

Escolha uma opção:

- Verdadeiro ✔
- Falso

A resposta correta é 'Verdadeiro'.

Questão **8**

Correto

Atingiu 1,00 de 1,00

É ou são vantagens de NIDS:

- a. Não interfere nos fluxos da rede. ✔
- b. Identifica alteração no sistema de arquivos. ✖
- c. Ajuda na segurança de vários hosts da rede. ✔
- d. Pode ser invisível na rede. ✔
- e. Identifica usuários e processos maliciosos. ✖

Sua resposta está correta.

As respostas corretas são:
Ajuda na segurança de vários hosts da rede.,

Pode ser invisível na rede.,

Não interfere nos fluxos da rede.

Questão **9**

Correto

Atingiu 1,00 de 1,00

É ou são exemplos de HIDS:

- a. Suricata ✖
- b. OSSEC ✔
- c. AIDE ✔
- d. Snort ✖

Sua resposta está correta.

As respostas corretas são:
OSSEC,

AIDE

Questão **10**

Correto

Atingiu 1,00 de 1,00

É ou são vantagens de HIDS:

- a. Não apresentam problemas com switches. ✔
- b. São invisíveis na rede. ✖
- c. Pode detectar processos ou usuários maliciosos. ✔
- d. Um HIDS pode monitorar vários hosts. ✖

Sua resposta está correta.

As respostas corretas são:
Não apresentam problemas com switches.,

Pode detectar processos ou usuários maliciosos.

Questão **11**

Correto

Atingiu 1,00 de 1,00

O que significa IDS?

- a. Intrusion Detection System ✔
- b. Ivasion Detection System
- c. Inspect Detection System
- d. Intruder Detection System

Sua resposta está correta.

A resposta correta é:
Intrusion Detection System

Questão **12**

Correto

Atingiu 1,00 de 1,00

Falso negativo ✔ é quando acontece um ataque o e IDS não identifica o mesmo, ou seja, o ataque ocorre e nenhum alerta é gerado.

Sua resposta está correta.

A resposta correta é:
[Falso negativo] é quando acontece um ataque o e IDS não identifica o mesmo, ou seja, o ataque ocorre e nenhum alerta é gerado.

Questão **13**

Correto

Atingiu 1,00 de 1,00

Uma assinatura é composta por uma seqüência de bytes que representam um ataque. Quando é encontrado no trafego da rede algum código que seja idêntico às assinaturas, é uma provável indicação de ataque. Os SDI utilizam esta abordagem para a detecção de intrusão, através da utilização de expressões regulares, análise de contexto ou linguagens de assinatura, os pacotes de rede são analisados e comparados com uma base de dados de assinaturas. Um exemplo de assinatura seria a string `/etc/shadow` na qual, qualquer pacote de rede utilizando por exemplo, Telnet, que apresente um conjunto de caracteres similares à este, irá gerar um alerta, como por exemplo com o comando: `cat /etc/shadow` .

Escolha uma opção:

- Verdadeiro ✔
- Falso

A resposta correta é 'Verdadeiro'.

◄ Sondagem Quebra de Senhas (28/04/2023)

Seguir para...

Sondagem - VPN (30/05/2023) ►