ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5

Terminar revisão

Iniciado em	domingo, 8 set. 2024, 17:52
Estado	Finalizada
Concluída em	domingo, 8 set. 2024, 18:08
Tempo empregado	15 minutos 34 segundos

QUESTÃO 1

Correto

Vale 1,00 ponto(s).

Qual o primeiro passo que deve ser realizado em um teste de invasão?

Escolha uma opção:

a. Encontrar vulnerabilidades na aplicação, para convencer o cliente de que o teste é necessário.

b. Explorar vulnerabilidades que se sabe existir no ambiente.

c. Solicitar código-fonte da aplicação para realização de inspeção de código.

d. Obter autorização por escrito para realização do teste e o escopo que será coberto pela atividade. ✓

e. Realizar o mapeamento da aplicação.

Sua resposta está correta.

Um Pentester deve sempre ter uma autorização por escrito para realizar o seu trabalho sendo que esta autorização deve informar qual escopo e concordar com eventuais consequências do teste (inclusive situações jurídicas).

Solicitar acesso ao código fonte da aplicação seria uma segunda etapa a depender do escopo do teste.

Os demais itens refere-se a atividades que seriam executadas por

hackers para conseguir algum tipo de vantagem.

A resposta correta é: Obter autorização por escrito para realização do teste e o escopo que será coberto pela atividade.

QUESTÃO 2

Correto

Vale 1,00 ponto(s).

Assinale o item que normalmente pode ser identificado por varredores de vulnerabilidades:

Escolha uma opção:

a. Falhas na lógica de negócio.

b. Portas abertas em servidores. ✓

c. Uso inadequado de criptografia.

d. Falhas no controle de acesso.

e. Problemas que requerem entendimento semântico da aplicação.

Sua resposta está correta.

Varredores de vulnerabilidades buscam identificar falhas relacionadas a um determinado serviço e, para isso, sua primeira atividade é identificar as portas abertas em um host e analisar os banners dos serviços ativos.

A resposta correta é: Portas abertas em servidores.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

A empresa XPTO S/A deseja realizar um teste de invasão no seu ambiente e ao contratar um Pentester para realizá-lo foi definido que este não teria acesso a nenhuma informação, que não as divulgadas em canais oficiais, e que os próprios colaboradores não seriam notificados do teste que seria realizado. De acordo com este cenário estamos falando de um teste de invasão:

Escolha uma opção:

- a. caixa preta ✓
- b. caixa cinza
- c. caixa branca
- d. caixa azul

Sua resposta está correta.

Em um teste caixa branca o Pentester terá acesso a qualquer informação que necessitar. No caixa cinza apenas lhe será dado algum tipo de informação mais privilegiada enquanto no caixa preta ele deverá realizar o teste sem qualquer contato ou informação adicional.

Caixa azul não existe na literatura.

A resposta correta é: caixa preta

QUESTÃO 4

Incorreto

Vale 1,00 ponto(s).

Durante a realização de testes de invasão um Pentester irá fazer uso de várias ferramentas, metodologias e técnicas com o objetivo de comprometer o ambiente avaliado. Neste cenário avalias as assertivas abaixo:

I - Ao realizar o Pivotamento o Pentester busca obter maior controle sobre o ambiente.

II - O Pivoteamento é a última etapa que será executada por um Pentester

III - Durante o reconhecimento o Pentester irá buscar uma forma de persistir o acesso que ele eventualmente tenha conseguido ao ambiente

É correto o que se afirma em:

Escolha uma opção:

a. I apenas ✗

b. II apenas

c. Todas são falsas

d. II apenas

Sua resposta está incorreta.

No pivotamento o Pentester buscar comprometer uma máquina

central e a partir dela comprometer o resto do ambiente

A persistência é a última etapa realizada por um Pentester.

No reconhecimento o Pentester tem como objetivo apenas identificar mais informações sobre o alvo para facilitar o seu ataque. Manter o seu acesso (persistir) é a etapa final de um ataque.

A resposta correta é: Todas são falsas

QUESTÃO 5

Correto

Vale 1,00 ponto(s).

Os proxies de interceptação são uma das ferramentas mais utilizadas em testes de invasão de aplicações web. Com estas ferramentas é possível:

Escolha uma opção:

a. realizar a captura de pacotes que trafegam em uma rede.

b. inspecionar requisições e respostas HTTP e alterá-las conforme desejado, em tempo real. ✓

c. realizar varreduras de vulnerabilidades em um determinado host.

d. comprometer a segurança no trânsito e armazenamento de informações.

Sua resposta está correta.

Proxy de Interceptação são utilizados para inspecionar requisições e respostas HTTP e alterá-las conforme desejado, em tempo real.

Sniffers são utilizados para realizar a captura de pacotes que trafegam em uma rede.

Scanner de vulnerabilidades são utilizados para identificar falhas de segurança em um host.

Ataques men-in-the-middle são utilizados para comprometer a

segurança de dados em trânsito.

A resposta correta é: inspecionar requisições e respostas HTTP e alterá-las conforme desejado, em tempo real.

◄ Tarefa 2

Conteúdo do Módulo ►