Sua AVS aqui!

avalie seus conhecimentos

RETORNAR À AVALIAÇÃO

ARA0076 - SEGURANÇA CIBERNÉTICA 2023.2 (AVS)
Aluno: GABRIEL MOURA GUIMARÃES
Data: 27/11/2023 20:22:30 202302332137

1. Veja abaixo, **todas** as suas respostas gravadas no nosso banco de dados.
2. Caso você queira voltar à avaliação clique no botão "**Retornar à Avaliação**".
3. Caso queira **FINALIZAR** a avaliação, **digite o código de 4 carateres** impresso abaixo.

ATENÇÃO: Caso finalize esta avaliação você não poderá mais modificar as suas respostas.

NORJ Confirmar Código: NORJ FINALIZAR

Obs.: Os caracteres da imagem ajudam a Instituição a evitar fraudes, que dificultam a gravação das respostas.

1ª Questão

Respondido em 27/11/2023 20:09
Ref.: 202310205342

O mapeamento das vulnerabilidades também é muito importante para **evitar os ataques DDoS,** que ocorrem quando há sobrecarga em um serviço ou largura de banda de uma infraestrutura para torná-lo indisponível. Além disso, provoca o uso de recursos até seu total esgotamento ou explora a falha de um software para controlar o equipamento. Para evitar as ameaças, o ideal é mapear a vulnerabilidade. Assinale a alternativa correta!

- [x] Contar com um firewall;
- [ ] Fazer backup de sistemas e dados;
- [ ] Ter políticas de senhas para fazer o controle de acesso;
- [ ] Usar mecanismos anti-spam.
- [ ] Todas estão corretas.

2ª Questão

Respondido em 27/11/2023 19:57
Ref.: 202310364201

Quando vimos que as organizações devem implementar um plano de resposta a incidentes, para que elas possam lidar com os incidentes ocorridos de forma rápida e eficiente, e com o mínimo de danos possíveis, aprendemos que as mesmas devem executar alguns passos. Abaixo estão alguns desses passos, **EXCETO** um. Marque essa alternativa:

- [x] Treinar somente se necessário.
- [ ] Estabelecer os procedimentos necessários.
- [ ] Identificar e priorizar os ativos.
- [ ] Configurar uma equipe de resposta.
- [ ] Identificar os riscos potenciais.

3ª Questão

Respondido em 27/11/2023 19:58
Ref.: 202310203022

Em relação à segurança da informação, no caso de recuperação de Desastres, qual das opções abaixo tem objetivo é promover a disponibilidade de recursos para recuperação de dados?

- [ ] d) Restauração
- [ ] c) Disposição
- [x] b) Backup
- [ ] a) Armazenamento

☐ e) Sustentação

4ª Questão

Respondido em 27/11/2023 19:46
Ref.: 202310153006

Para analisar a anatomia de um ataque, precisamos entender os tipos de pessoas que efetuam esses ataques. Existe um grupo dessas pessoas de baixo conhecimento técnico que utilizam de scripts, tutoriais e ferramentas disponíveis na Internet para invadir sistemas. Essas pessoas são as:

☐ Crackers
☐ Insiders
☐ White Rackers
☐ Rackers
☒ Script Kiddies

5ª Questão

Respondido em 27/11/2023 20:11
Ref.: 202310148850

A segurança da informação deve existir para proteger os recursos de informação que são utilizados para o funcionamento de uma organização. Para essa proteção, algumas premissas devem ser observadas e estudadas. Abaixo citamos algumas, **EXCETO** uma. Marque essa opção:

☐ a. Conhecer os possíveis oponentes.

☐ a. Considerar os fatores humanos.

☐ a. Conhecer os pontos fracos da empresa.

☐ a. Contabilizar os valores.

☒ Aplicar a segurança de acordo com o que o conselho da empresa decidir.

6ª Questão

Respondido em 27/11/2023 20:16
Ref.: 202310153258

O termo ¿hardening¿ de sistemas consiste numa coleção de técnicas utilizadas, ferramentas e práticas recomendadas, com o objetivo de reduzir as vulnerabilidades em *softwares*, sistemas e em toda a infraestrutura da empresa. A ideia é reduzir os riscos de segurança, eliminando ou limitando os vetores de ataques em potencial. Algumas etapas devem ser seguidas para que se alcance esse objetivo. Abaixo listamos exemplos corretos dessas etapas, EXCETO um. Marque essa alternativa:

☒ Verificação da compatibilidade em ambiente de produção.
☐ Escolha de um Nível de Implementação para o "hardening".
☐ Escolha de um Guia de Referência para o "hardening".
☐ Verificação se o "hardening" está atualizado.
☐ Verificação da compatibilidade dos procedimentos de Rollback.

7ª Questão

Respondido em 27/11/2023 20:16
Ref.: 202310364855

Hardening é o processo de tornar os sistemas, redes, softwares, hardwares e firmwares, bem como infraestruturas de TI mais resistentes a ataques. O Hardening envolve a implementação de medidas de segurança preventiva, como a criptografia, protocolos de autenticação e autorização, instalação de firewalls, segmentação de redes e controle de acesso físico. Geralmente é aplicado em etapas. Abaixo algumas dessas etapas são listadas, porém uma delas não está correta. Marque essa opção **INCORRETA**:

☒ Avaliação do ecossistema.
☐ Revisão dos processos de transferência de dados.
☐ Fortalecimento da política de criação de senhas e proteção de contas.
☐ Automatização de patches e atualizações.
☐ Escolher a criptografia como uma opção de segurança.

8ª Questão

Respondido em 27/11/2023 20:17
Ref.: 202310130161

A sigla OWASP é a abreviação para ¿Open Web Application Security Project¿. Trata-se de uma entidade sem fins lucrativos e com reconhecimento internacional, atuando com foco na colaboração para o fortalecimento da segurança de softwares em todo o mundo. O OWASP mantém uma lista com as 10 falhas de segurança de aplicativos da Web mais perigosas, juntamente com os métodos mais eficazes para lidar com elas.

Sobre este assunto, marque a opção incorreta:

☒ As melhores práticas pregadas pelo OWASP ajudam a tornar as aplicações mais blindadas contra ataques cibernéticos, entretanto não colabora para a redução do índice de erros e falhas operacionais nos sistemas;
☐ O OWASP é um projeto de comunidade de segurança gratuita e aberta, que fornece muitos conhecimentos e ferramentas para ajudar qualquer pessoa envolvida nos processos de criação, desenvolvimento, testes, implementação e suporte de uma aplicação web a garantir que a segurança seja constituída desde o início e que o produto final seja tão seguro quanto possível
☐ O grupo que sustenta o projeto é composto por uma gama de especialistas em segurança na web espalhados por todo o mundo. Eles compartilham seus conhecimentos e experiências sobre as vulnerabilidades, ameaças, ataques e contramedidas existentes.

- [ ] O OWASP tem como ideia central reunir as informações mais importantes que permitam a avaliação dos riscos de segurança e as formas de combatê-las eficientemente.
- [ ] O OWASP contribui para uma codificação (criptografias) mais forte e eleva o potencial de sucesso das aplicações;

9ª Questão

Respondido em 27/11/2023 20:18
Ref.: 202308414476

Existem muitos riscos bem conhecidos e de domínio público que são úteis como fontes de referências para que pesquisadores e desenvolvedores aprendam como identificá-los e evitar que estejam presentes nos sistemas. Uma das fontes mais conhecidas é o Top 10 da OWASP (OWASP Top Ten, 2020). Trata-se de um relatório que descreve os principais riscos de segurança de aplicativos da web. O foco do relatório está nas dez principais vulnerabilidades e é atualizado regularmente. Assim, o risco de segurança que corre quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta legítima. Os dados hostis do atacante podem enganar o interpretador levando-o a executar comandos não pretendidos ou a aceder a dados sem a devida autorização (Adaptado OWASP Top 2017). Este risco de segurança é conhecido como:

- [ ] Quebra de Controle de Acessos
- [ ] Quebra de Autenticação
- [x] Injeção
- [ ] Entidades Externas de XML (XXE)
- [ ] Exposição de Dados

10ª Questão

Respondido em 27/11/2023 20:21
Ref.: 202310126285

A segurança cibernética tem como mitigar as chances de ataques bem sucedidos em qualquer organização. Dentro deste contexto, analise as asserções e abaixo e marque a opção que explicita quais as afirmações estão corretas:

I - A Segurança cibernética tem como objetivo dissuadir, prevenir, detectar e responder a ataques advindos do espaço cibernético.

II - Espaço cibernético constitui-se basicamente pela rede mundial de computadores ¿ Internet ¿ onde os dados transitam.

III - Todos os ataques cibernéticos têm como origem a Internet

- [ ] Apenas III
- [ ] Apenas II
- [ ] Apenas I
- [x] Apenas I e II
- [ ] Apenas I e III