UniCesumar
EDUCAÇÃO A DISTÂNCIA

PROJETO DE ENSINO - PENTEST E RED TEAM-SEGREDOS DA SEGURANÇA CIBERNÉTICA - 53_2025

Período:23/07/2025 08:00 a 21/09/2025 23:59 (Horário de Brasília)
Status:ABERTO
Gabarito: Gabarito será liberado no dia 22/09/2025 00:00 (Horário de Brasília)

1ª QUESTÃO

A segurança da informação se dedica a proteger os dados e informações de organizações contra ameaças e ataques cibernéticos. Ela engloba a implementação de medidas e políticas que visam garantir a confidencialidade, integridade e disponibilidade dos dados, bem como a prevenção de acesso não autorizado, modificação ou destruição dos mesmos.

Fonte: SILVA, R.F.; PEREIRA, J.C. **Identificando vulnerabilidades de segurança computacional.** 2013. Disponível em: < https://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf >. Acesso em: 16 maio 2024.

De acordo com o artigo “Identificando vulnerabilidades de segurança computacional.”, de Raquel Fonseca da Silva e Julio César Pereira (2013), responda qual é o método utilizado para explorar as falhas e fraquezas dos sistemas computacionais, aproveitando-se da vulnerabilidade humana. Analise as afirmativas abaixo e assinale a correta:

ALTERNATIVAS

- Firewall.
- Antivírus.
- Criptografia.
- Engenharia Social.
- Autenticação de dois fatores.

2ª QUESTÃO

Segundo o trabalho de conclusão de curso “A importância do Pentest para os negócios de uma empresa”, de Roberto de Carvalho Piconi (2016):

As medidas de segurança da informação são essenciais para proteger as informações de uma organização contra ameaças e garantir sua confidencialidade, integridade e disponibilidade. É importante que as organizações apliquem um conjunto abrangente de medidas de segurança da informação para garantir a proteção adequada dos seus ativos e minimizar os riscos de violações de segurança.

Fonte: PICONI, Roberto de Carvalho. **A importância do Pentest para os negócios de uma empresa, 2016**. Trabalho de conclusão de curso (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2016. Disponível em: < https://ric.cps.sp.gov.br/handle/123456789/399 >. Acesso em: 16 maio 2024.

Sobre as medidas de segurança mencionadas no texto, avalie as afirmativas a seguir.

I. As medidas de segurança mencionadas por Sêmola (2003, p. 49) são apenas corretivas, não possuindo características preventivas ou detectáveis.
II. As medidas preventivas visam evitar incidentes, através de políticas de segurança, normas, procedimentos e outras práticas.
III. As medidas detectáveis têm como objetivo identificar ameaças e impedir a exploração de vulnerabilidades.
IV. As medidas corretivas não são eficazes para corrigir falhas na estrutura tecnológica e humana.
V. As medidas de segurança têm como objetivo proteger as informações e os ativos da organização contra ameaças que possam explorar suas vulnerabilidades.

É correto apenas o que se afirma em:

ALTERNATIVAS

- I.
- I e II.
- II, III e V.
- II, IV e V.
- II, III, IV e V.

3ª QUESTÃO

Segundo a monografia “Análise e Testes de Intrusão em Dispositivos IoT”, de Jhonny Oliveira da Silva (2023):

A proteção da rede de internet residencial é essencial para garantir a segurança dos dispositivos e dados pessoais conectados à rede. Existem várias medidas que podem ser tomadas para fortalecer a proteção da rede residencial. A falta de proteção adequada da rede pode resultar em consequências graves, como acesso não autorizado a informações confidenciais, ataques de malware, roubo de identidade, comprometimento da privacidade, perda de dados, interrupção dos serviços e danos à reputação. É fundamental implementar medidas de segurança para evitar essas consequências e garantir a proteção da rede residencial.

Fonte: SILVA, Jhonny Oliveira. **Análise e testes de intrusão em dispositivos IoT. 2023. 76 f**. Monografia (Graduação em Engenharia de Computação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2023. Disponível em: < https://monografias.ufop.br/handle/35400000/5568 >. Acesso em: 16 maio 2024.

De acordo com sua leitura responda qual é o primeiro passo para garantir a segurança da sua rede residencial? Analise as afirmativas abaixo e assinale a correta:

ALTERNATIVAS

- Desativar completamente o roteador.
- Contratar um serviço de antivírus pago.
- Verificar a velocidade da conexão com a internet.
- Conectar-se a redes Wi-Fi públicas sem proteção.
- Realizar uma verificação das portas abertas e desprotegidas no roteador de borda.

4ª QUESTÃO

De acordo com a monografia “Análise e Testes de Intrusão em Dispositivos IoT”, de Jhonny Oliveira da Silva (2023), temos que a segurança em Internet das Coisas (IoT) é um tema de extrema importância na era digital em que vivemos. Com o crescente número de dispositivos conectados, como eletrodomésticos inteligentes, veículos autônomos e sistemas de monitoramento, a proteção dos dados e a segurança das redes se tornaram preocupações primordiais.

Fonte: SILVA, Jhonny Oliveira. **Análise e testes de intrusão em dispositivos IoT. 2023. 76** f. Monografia (Graduação em Engenharia de Computação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2023. Disponível em: < https://monografias.ufop.br/handle/35400000/5568 >. Acesso em: 16 maio 2024.

Nesse contexto, destacam-se os requisitos de segurança mais importantes, definidos como a Tríade da Segurança da Informação, as quais são:

ALTERNATIVAS

- Trojans, worms e vírus.
- Ataques físicos, de rede e de software.
- Disponibilidade, autenticidade e criptografia.
- Confidencialidade, integridade e disponibilidade.
- Vírus, spyware e ataques de negação de serviço.

5ª QUESTÃO

A segurança na rede e nos computadores é essencial para proteger os dados e a privacidade. Isso envolve o uso de firewalls para controlar o tráfego de rede, a criptografia para proteger as informações durante a transmissão, a autenticação para verificar a identidade dos usuários, o controle de acesso para limitar o acesso aos recursos da rede, o monitoramento contínuo para detectar atividades suspeitas, além de manter os sistemas atualizados, utilizar antivírus e antimalware, criar senhas fortes, realizar backups de dados e conscientizar os usuários sobre as práticas de segurança.

Fonte: SILVA, R.F.; PEREIRA, J.C. **Identificando vulnerabilidades de segurança computacional.** 2013. Disponível em: < https://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf >. Acesso em: 16 maio 2024.

A partir da leitura do artigo “Identificando vulnerabilidades de segurança computacional.”, de Raquel Fonseca da Silva e Julio César Pereira (2013), é definido o conceito de “*pentesting*”. Assim, podemos afirmar que a função do *pentesting* é:

ALTERNATIVAS

- Facilitar a compreensão das regras pelos desenvolvedores e pesquisadores.
- Desenvolver softwares maliciosos para explorar vulnerabilidades em sistemas operacionais.
- Realizar a manutenção preventiva dos sistemas computacionais para evitar ataques cibernéticos.
- Criar novos sistemas de segurança para proteger os sistemas computacionais contra ameaças externas.
- Avaliar a segurança dos sistemas computacionais ou rede, simulando ataques e buscando suas indefesas.

6ª QUESTÃO

Desenvolvimento de aplicações web seguras é uma área crucial no mundo digital atual. Com o aumento das ameaças cibernéticas, garantir a segurança das aplicações web se tornou uma prioridade para empresas e desenvolvedores. Essa área envolve uma abordagem proativa, com atualizações constantes, monitoramento e análise de vulnerabilidades, garantindo assim uma experiência confiável e segura para os usuários.

Fonte: TIMÓTEO, Lívia Ester Felipusso. Políticas de segurança da informação alinhadas a ISO 27001 com base na OWASP top 10 aplicadas à gerência de projetos para aplicações web. 2023. Trabalho de conclusão de curso Ciências Exatas e da Terra: Ciência da Computação: Sistemas de Computação - Instituto Federal Goiano, Morrinhos, 2023. Disponível em: < https://repositorio.ifgoiano.edu.br/handle/prefix/3850 >. Acesso em: 16 maio 2024.

A partir da leitura do trabalho de conclusão de curso “Políticas de segurança da informação alinhadas a ISO 27001 com base na OWASP top 10 aplicadas à gerência de projetos para aplicações web” (Timóteo, 2023), responda como a gerência de projetos, aliada a PSIs, OWASP e ISOs 27001 e 27002, podem contribuir para o desenvolvimento de aplicações web seguras?

ALTERNATIVAS

- Oferecendo suporte exclusivo para iniciantes no mercado de trabalho.
- Implementar medidas de segurança física para proteger dados na web.
- Facilitando o processo de tomada de decisão para a produtividade e desempenho dos projetos.
- Proporcionando somente uma base sólida de conhecimento teórico para os profissionais de segurança.
- As PSIs, OWASP e ISOs 27001 e 27002 não são relevantes para garantir a segurança das aplicações web.

7ª QUESTÃO

A segurança computacional é uma área que se concentra na proteção dos sistemas de computadores e redes contra ameaças cibernéticas. Ela envolve a implementação de medidas e práticas para prevenir ataques, proteger dados e garantir a integridade e disponibilidade dos sistemas. Ela é um desafio contínuo, pois as ameaças cibernéticas estão em constante evolução. Portanto, é importante manter-se atualizado com as últimas tendências e melhores práticas de segurança, além de implementar uma abordagem em camadas para proteger os sistemas e dados contra ameaças cada vez mais sofisticadas.

Fonte: SILVA, R.F.; PEREIRA, J.C. **Identificando vulnerabilidades de segurança computacional.** 2013. Disponível em: < https://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf >. Acesso em: 16 maio 2024.

A partir da leitura do artigo “Identificando vulnerabilidades de segurança computacional.”, de Raquel Fonseca da Silva e Júlio César Pereira (2013), assinale a alternativa que apresenta a melhor maneira de manter as informações seguras, evitando que sejam violadas ou comprometidas.

ALTERNATIVAS

- Ignorar a segurança das informações.
- Contar com a sorte para evitar invasões.
- Fazer backups regulares das informações.
- Criptografar as informações após a violação ocorrer.
- Proteger as informações antes que ocorra a violação.

8ª QUESTÃO

A segurança de dados e da informação é um aspecto fundamental na era digital em que vivemos. Com o crescente avanço da tecnologia, a quantidade de dados e informações que são armazenados e transmitidos diariamente aumentou significativamente. Nesse contexto, a proteção desses dados se tornou uma preocupação essencial para empresas e indivíduos. A segurança de dados envolve a implementação de medidas e práticas para garantir a confidencialidade, integridade e disponibilidade das informações.

Fonte: PICONI, Roberto de Carvalho. **A importância do Pentest para os negócios de uma empresa,** 2016. Trabalho de conclusão de curso (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2016. Disponível em: < https://ric.cps.sp.gov.br/handle/123456789/399 >. Acesso em: 16 maio 2024.

A partir da leitura do trabalho de conclusão de curso “A importância do Pentest para os negócios de uma empresa”, de Roberto de Carvalho Piconi (2016), analise as afirmações a seguir.

I. Todos os sistemas são 100% seguros e não possuem pontos fracos.
II. Com o avanço da tecnologia, surgem constantemente novas formas de uso, acompanhadas por novas falhas.
III. As ameaças são agentes ou condições que podem comprometer os ativos das empresas ao explorar vulnerabilidades.
IV. As ameaças naturais estão relacionadas a fenômenos da natureza, como alagamentos e terremotos.
V. As ameaças voluntárias são causadas intencionalmente por seres humanos, como hackers, espiões e ex-funcionários.

É correto apenas o que se afirma em:

ALTERNATIVAS

- I.
- I e II.
- II, III e V.
- II, IV e V.
- II, III, IV e V.

9ª QUESTÃO

A segurança da informação na web é de extrema importância para proteger dados sensíveis e garantir a privacidade dos usuários. Com o crescente número de ameaças cibernéticas, é essencial implementar medidas de segurança eficazes. Isso inclui o uso de firewalls, criptografia de dados, autenticação de dois fatores e atualizações regulares de software. Além disso, é fundamental educar os usuários sobre práticas seguras, como evitar o compartilhamento de informações pessoais sensíveis e o uso de senhas fortes. A colaboração entre empresas, governos e usuários é essencial para manter a segurança da informação na web e garantir a confiança dos usuários ao navegar e realizar transações online.

Fonte: TIMÓTEO, Lívia Ester Felipusso. **Políticas de segurança da informação alinhadas a ISO 27001 com base na OWASP top 10 aplicadas à gerência de projetos para aplicações web.** 2023. Trabalho de conclusão de curso Ciências Exatas e da Terra: Ciência da Computação: Sistemas de Computação - Instituto Federal Goiano, Morrinhos, 2023. Disponível em: < https://repositorio.ifgoiano.edu.br/handle/prefix/3850 >. Acesso em: 16 maio 2024.

A partir da leitura do trabalho de conclusão de curso “Políticas de segurança da informação alinhadas a ISO 27001 com base na OWASP top 10 aplicadas à gerência de projetos para aplicações web.”, Lívia Ester Felipusso (2023), escolha qual é a alternativa que apresenta o objetivo principal das Políticas de Segurança da Informação.

ALTERNATIVAS

- Estabelecer diretrizes para a proteção de sistemas de pagamento online.
- Prevenir incidentes de segurança por meio de normas, regras e ferramentas.
- Garantir a segurança de transações financeiras em aplicativos de mensagens.
- Definir políticas de segurança física para a proteção de instalações corporativas.
- Garantir a confidencialidade de dados em sistemas de armazenamento especificamente em nuvem.

10ª QUESTÃO

A segurança de rede é um aspecto fundamental para garantir a proteção dos dados e informações que transitam em uma rede de computadores. Ela envolve a implementação de medidas e protocolos para prevenir ataques cibernéticos, proteger a privacidade dos usuários e garantir a integridade dos sistemas. No contexto da Internet das Coisas (IoT), a segurança também é uma preocupação importante. Os dispositivos conectados à IoT estão cada vez mais presentes em nossas vidas, desde eletrodomésticos inteligentes até sistemas de segurança residencial. No entanto, esses dispositivos podem apresentar vulnerabilidades de segurança que podem ser exploradas por hackers.

Fonte: SILVA, Jhonny Oliveira. **Análise e testes de intrusão em dispositivos IoT.** 2023. 76 f. Monografia (Graduação em Engenharia de Computação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2023. Disponível em: < https://monografias.ufop.br/handle/35400000/5568 >. Acesso em: 16 maio 2024.

A partir da leitura da monografia “Análise e Testes de Intrusão em Dispositivos IoT”, de Jhonny Oliveira da Silva (2023), assinale qual alternativa apresenta as principais vulnerabilidades identificadas nos dispositivos testados em relação ao top 5 da Owasp.

ALTERNATIVAS

- Interfaces Web seguras em impressoras e roteadores mesh.
- Menor possibilidade de ataque em interruptores inteligentes e TVs inteligentes.
- Presença de serviços seguros e senhas robustas em roteadores de borda e Mikrotik.
- Falta de criptografia em roteadores mesh e vazamento de informações confidenciais do usuário.
- Exploração bem-sucedida e segura do serviço de salvamento de informações da Google Nest Mini.