Universidade Virtual Africana

INFORMÁTICA APLICADA: CSI 3303

INTRODUÇÃO À SEGURANÇA INFORMÁTICA

Gilberto Antonio Luis

Prefácio

A Universidade Virtual Africana (AVU) orgulha-se de participar do aumento do acesso à educação nos países africanos através da produção de materiais de aprendizagem de qualidade. Também estamos orgulhosos de contribuir com o conhecimento global, pois nossos Recursos Educacionais Abertos são acessados principalmente de fora do continente africano.

Este módulo foi desenvolvido como parte de um diploma e programa de graduação em Ciências da Computação Aplicada, em colaboração com 18 instituições parceiras africanas de 16 países. Um total de 156 módulos foram desenvolvidos ou traduzidos para garantir disponibilidade em inglês, francês e português. Esses módulos também foram disponibilizados como recursos de educação aberta (OER) em oer.avu.org.

Em nome da Universidade Virtual Africana e nosso patrono, nossas instituições parceiras, o Banco Africano de Desenvolvimento, convido você a usar este módulo em sua instituição, para sua própria educação, compartilhá-lo o mais amplamente possível e participar ativamente da AVU Comunidades de prática de seu interesse. Estamos empenhados em estar na linha de frente do desenvolvimento e compartilhamento de recursos educacionais abertos.

A Universidade Virtual Africana (UVA) é uma Organização Pan-Africana Intergovernamental criada por carta com o mandato de aumentar significativamente o acesso a educação e treinamento superior de qualidade através do uso inovador de tecnologias de comunicação de informação. Uma Carta, que estabelece a UVA como Organização Intergovernamental, foi assinada até agora por dezenove (19) Governos Africanos - Quênia, Senegal, Mauritânia, Mali, Costa do Marfim, Tanzânia, Moçambique, República Democrática do Congo, Benin, Gana, República da Guiné, Burkina Faso, Níger, Sudão do Sul, Sudão, Gâmbia, Guiné-Bissau, Etiópia e Cabo Verde.

As seguintes instituições participaram do Programa de Informática Aplicada: (1) Université d'Abomey Calavi em Benin; (2) Université de Ougagadougou em Burkina Faso; (3) Université Lumière de Bujumbura no Burundi; (4) Universidade de Douala nos Camarões; (5) Universidade de Nouakchott na Mauritânia; (6) Université Gaston Berger no Senegal; (7) Universidade das Ciências, Técnicas e Tecnologias de Bamako no Mali (8) Instituto de Administração e Administração Pública do Gana; (9) Universidade de Ciência e Tecnologia Kwame Nkrumah em Gana; (10) Universidade Kenyatta no Quênia; (11) Universidade Egerton no Quênia; (12) Universidade de Addis Abeba na Etiópia (13) Universidade do Ruanda; (14) Universidade de Dar es Salaam na Tanzânia; (15) Universite Abdou Moumouni de Niamey no Níger; (16) Université Cheikh Anta Diop no Senegal; (17) Universidade Pedagógica em Moçambique; E (18) A Universidade da Gâmbia na Gâmbia.

Bakary Diallo

O Reitor

Universidade Virtual Africana

Créditos de Produção

Autor

Gilberto Antonio Luis

Par revisor(a)

Ambrosio Vumo

UVA - Coordenação Académica

Dr. Marilena Cabral

Coordenador Geral Programa de Informática Aplicada

Prof Tim Mwololo Waema

Coordenador do módulo

Robert Oboko

Designers Instrucionais

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Equipa Multimédia

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Direitos de Autor

Apoiado por

Projeto Multinacional II da UVA financiado pelo Banco Africano de Desenvolvimento..

Tabela de conteúdo

Descrição Geral do Curso

Bem-vindo(a) a [Introdução á Segurança Informática]

O módulo de introdução á segurança informática fornece uma possibilidade de um estudo essencial das questões de segurança de informática. Concentra-se em todos os processos e mecanismos pelos quais os sistemas computacionais, informação, bem como os serviços estão protegidos contra utilizadores não autorizados.

Finalizando este módulo, os(as) estudantes terão conceitos fundamentais de segurança do computador e serão capazes de projetar e desenvolver sistemas de autenticação e sistemas de segurança.

Este módulo possibilita ainda a aprendizagem de métodos e ferramentas em segurança de computadores e permite que os (as) estudantes também aprendem a proteger suas operações num ambiente de rede.

Pré-requisitos

- Introdução á Informática.
- Redes de Computadores e Comunicação de Dados.

Materiais

Os materiais necessários para completar este curso incluem:

- Laptops, Smart Phones, IPTV, Video Conferência.

Bibliografia:

- Torres, C. B., Silva, P. T., Carvalho, H., "Segurança dos Sistemas de Informação. Gestão Estratégica da Segurança Empresarial." Edições Centro Atlântico, 2003.
- Monteiro, E., Boavida, F., "Engenharia de Redes Informáticas". 10a Edição Actualizada e Aumentada, Editora FCA, 2011.
- Malik, S., "Network Security Principles and Practices". Cisco Press. 2002.
- Mark Rhodes-Ousley, et al. "Network Security: The Complete Reference," 2003.
- MOREIRA, Stringasci Nilton; Segurança Mínima: uma visão coorporativa da segurança de Informações; Rio de Janeiro; Axcel Books; 2001.
- Kaufman, C., et al., "Network Security: Private Communication in a Public World". 2ed., Prentice Hall, 2002.
- Gert DeLaet, Gert Schauwers, "Network Security Fundamentals", Cisco Press Fundamentals Series, 2004
- Stallings, W., Criptografia e segurança de redes – Princípios e práticas, Editora Pearson Brasil. 4ª edição, 2008.
- Mamede, H. S, "Segurança Informática Nas Organizações", Editora: FCA, 2006.

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011.
- TANENBAUM, ANDREW S. Redes de Computadores. Ed. Pearson, 4ª edição, 2003.
- TANENBAUM, ANDREW S. Sistemas Operacionais Modernos. Ed. Pearson, 3ª edição, 2010.
- NORTON, P. Introdução à Informática. Makron Books. 1997.
- Monteiro, M. A. Introdução à Organização de Computadores. LTC. 1992.
- MEYER, M., BABER, R. e PFAFFENBERGER, B. Nosso Futuro e o Computador. Bookman. 1999.
- LANCHARRO, E. A. , LOPEZ, M. G. e FERNANDEZ, S. P. Informática básica. Makron Books. 1991.
- IDOETA, I. V. e CAPUANO, F. G. Elementos de Eletrônica Digital. Editora Érica.
- TANENBAUM, A. S. Organização Estruturada de Computadores. Quarta Edição. LTC. 2001.
- https://repositorio.ufba.br/ri/bitstream/ri/8183/1/Disserta%C3%A7%C3%A3o%20Bianka.pdf
- http://www.barbacena.com.br/tonmaster/downloads/Malware.pdf
- http://www.slideshare.net/alvaro_tando/apostila-versao-20
- http://www2.dbd.puc-rio.br/pergamum/tesesabertas/0410821_07_cap_03.pdf
- http://pt.wikipedia.org/w/index.

Objetivos do Curso

Após concluir este curso, o(a) estudante deve ser capaz de:

- Identificar e discutir os conceitos básicos de segurança informática;
- Entender a funcionalidade de autenticação e controle de acesso.
- Conceber uma rede de comunicação de dados segura, de acordo com o investimento assim como o nível de segurança requerido.
- Assumir a responsabilidade pela instalação, configuração e manutenção da segurança da rede.
- Identificar o impacto social da segurança informática no dia a dia, como por exemplo nas transações online, no e-commerce, dentre outras actividades que envolvem a utilização dos meios computacionais.
- Identificar as ameaças, ataques e vulnerabilidades em um ambiente informatizado.
- Conhecer os mecanismos e ferramentas de segurança informática.

Unidades

Unidade 0: Diagnóstico

Nesta unidade será aplicado um teste diagnóstico de modo a apurar o nivel de conhecimento dos(as) estudantes em relação ao curso.

Unidade 1: Conceitos Básicos de Segurança Informática

Nesta unidade serão abordados os conceitos básicos de segurança informática.

Unidade 2: Ameaças, Ataques , Vulnerabilidades e Mecanismos de segurança Informática.

Nesta unidade serão abordados os diferentes tipos de ameaças e ataques a que um sistema informático está vulnerável, bem como o estudo de alguns mecanismos de segurança informática.

Unidade 3: Software malicioso e software de Proteção.

Nesta unidade serão abordados os softwares maliciosos assim como os softwares para remoção dos mesmos.

Unidade 4: Serviços da Segurança Informática e Infraestrutura de segurança

Nesta unidade serão abordados os métodos de autenticação e algumas infraestrutura de segurança.

Avaliação Em cada unidade encontram-se incluídos instrumentos de avaliação formativa a fim de verificar o progresso do(a)s estudantes.

No final de cada módulo são apresentados instrumentos de avaliação sumativa, tais como testes e trabalhos finais, que compreendem os conhecimentos construidos e as competências desenvolvidas ao estudar este módulo.

A implementação dos instrumentos de avaliação sumativa fica ao critério da instituição que oferece o curso. A estratégia de avaliação sugerida é a seguinte:

1	[Questionários, Trabalhos prácticos]	20%
2	[Avaliação Contínua]	20%
4	Laboratório	20%
3	[Exame Final]	40%

Calendarização

Unidade	Temas e Atividades	Estimativa do tempo
[Unidade 1]	3 Avaliações	18 Horas
[Unidade 2]	7 Avaliações	18 Horas
[Unidade 3]	1 Avaliação	18 Horas
[Unidade 4]	4 Avaliações	72 Horas

Leituras e outros Recursos

As leituras e outros recursos deste curso são:

Unidade 0

Leituras e outros recursos obrigatórios:

- TANENBAUM, ANDREW S. Redes de Computadores. Ed. Pearson, 4ª edição, 2003.
- TANENBAUM, ANDREW S. Sistemas Operacionais Modernos. Ed. Pearson, 3ª edição, 2010.
- NORTON, P. Introdução à Informática. Makron Books. 1997.
- Monteiro, M. A. Introdução à Organização de Computadores. LTC. 1992.
- MEYER, M., BABER, R. e PFAFFENBERGER, B. Nosso Futuro e o Computador. Bookman. 1999.
- LANCHARRO, E. A. , LOPEZ, M. G. e FERNANDEZ, S. P. Informática básica. Makron Books. 1991.
- IDOETA, I. V. e CAPUANO, F. G. Elementos de Eletrônica Digital. Editora Érica.
- TANENBAUM, A. S. Organização Estruturada de Computadores. Quarta Edição. LTC. 2001.

Unidade 1

Leituras e outros recursos obrigatórios:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008.
- Mamede, H. S, "Segurança Informática Nas Organizações", Editora: FCA, 2006.
- Leituras e outros recursos opcionais:
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2
- https://pt.wikiversity.org/wiki/Seguran%C3%A7a_em_Redes_de_Dados/Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o

Unidade 2

Leituras e outros recursos obrigatórios:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Mamede, H. S, "Segurança Informática Nas Organizações", Editora: FCA, 2006.
- MOREIRA, Stringasci Nilton; Segurança Mínima: uma visão coorporativa da segurança de Informações; Rio de Janeiro; Axcel Books; 2001.
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011

Leituras e outros recursos opcionais:

- Monteiro, E., Boavida, F., "Engenharia de Redes Informáticas". 10a Edição Actualizada e Aumentada, Editora FCA, 2011.
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011

Unidade 3

Leituras e outros recursos obrigatórios:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Mamede, H. S, "Segurança Informática Nas Organizações", Editora: FCA, 2006.
- MOREIRA, Stringasci Nilton; Segurança Mínima: uma visão coorporativa da segurança de Informações; Rio de Janeiro; Axcel Books; 2001.

- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2

Leituras e outros recursos opcionais:

- http://www.peotta.com/sbseg2011/resources/downloads/minicursos/90650.pdf

Unidade 4

Leituras e outros recursos obrigatórios:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Monteiro, E., Boavida, F., "Engenharia de Redes Informáticas". 10a Edição Actualizada e Aumentada, Editora FCA, 2011.
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011.

Leituras e outros recursos opcionais:

- http://repositorium.sdum.uminho.pt/bitstream/1822/6712/1/Tese-Tecnologias%20de%20Seguran%C3%A7a%20no%20e-Vote.pdf
- http://www.portaleducacao.com.br/educacao/artigos/48819/ameacas-e%20vulnerabilidades-da-informacao-como-precaver

Unidade 0. Diagnóstico

Introdução à Unidade

O propósito desta unidade é verificar a compreensão dos conhecimentos que possui relacionados com este curso.

Estudantes:

Nesta seção você vai encontrar questões de auto-avaliação que irão ajudá-lo a testar sua prontidão para fazer este módulo. Você tem que encarar esta unidade como uma base para poder triunfar neste módulo.

Instrutores:

Questões de pré-avaliação fornecidos aqui levam os(as) estudantes a saber se eles estão preparados, no entanto, sugere-se que você incentive os (as) estudantes a avaliar-se, respondendo a todas as perguntas abaixo. Caso os estudantes dominem os pré-requisitos eles têm a base necessária para iniciar o Módulo.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

A seguir apresentam-se frases com várias alternativas de resposta. Deve escolher, em cada caso a alternativa correcta. Para verificar o seu nível de preparação poderá no fim comparar as suas respostas com a proposta de respostas no fim da unidade.

1. O termo técnico usado para designar a parte física do computador é :

   A. Software

   B. Hardware

   C. Periférico

   D. Modem

2. A CPU é a unidade responsável por (Escolher a afirmação correta):

   A. Ventilar o sistema

   B. Apresentar graficamente a informação.

   C. Executar as tarefas de processamento

   D. Substituir o teclado

3. O que é uma rede de computadores?

A. Conjunto de periféricos integrados.

B. Conjunto de computadores interligados entre si, compartilhando recursos.

C. União de equipamentos com a única finalidade de compartilhar internet.

D. Vários computadores que fazem parte dos setores de uma organização.

4. Quanto à dispersão geográfica como são classificadas as redes de computadores?

A. MAN, NAN, LAN

B. LAN, MAN, WAN

C. LAN, NAN, WAN

D. LAN, MAN, TAN

5. Quanto á topologia física, como são denominadas as redes?

A. Barra, Anular, Estrela e Token

B. Anel, híbrida, Estelar e Camada

C. Barramento, Anel, Estrela, Híbrida

D. Segmento, Híbrida, Estrela e Token

6. O que é a tecnologia Broadcast?

A. Transmissão simultânea para todos os hosts na rede.

B. Transmissão aleatória na rede.

C. Modo de transferência de arquivos mais rápido.

D. Modo de transferência de arquivos lento.

7. Dos equipamentos de rede abaixo, qual tem a função de escolher o melhor caminho para o envio da informação?

A. Switch

B. Roteador

C. Access Point

D. Patch Panel

8. Qual desses tipos de conexões cobrem cidades?

   A. MAN

   B. WAN

   C. LAN

   D. PAN

9. O que é P2P?

   A. Peer-to-Peer

   B. PHP

   C. Powerpoint

10. Quais destes são componentes de rede?

    A. Monitor, Rato e Teclado

    B. Processador, Memórias e Placa Gráfica

    C. Cabos, Hub, Router

Solução proposta:

1. B
2. C
3. B
4. B
5. C
6. A
7. B
8. B
9. A
10. C

Unidade 1. [Conceitos Básicos de Segurança Informática]

Introdução à Unidade

Nesta unidade serão abordados os conceitos básicos de segurança Informática incluindo os objectivos principais de segurança Informática, desafios de segurança Informática, e o modelo de segurança Informática.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Aplicar correctamente os conceitos-chave de segurança informática em situações concretas;
- Conhecer o modelo de segurança informática;
- Identificar os diferentes desafios de segurança informática.

Termos-chave

Confidencialidade: corresponde às informações estarem disponíveis somente a quem está devidamente autorizado a acedê-las.

Integridade: Diz respeito à informação estar intacta, sem quebras e sem alterações não autorizadas. Este ítem carrega em si outro que alguns autores chamam confiabilidade.

Disponibilidade: Diz respeito à informação estar disponível para o utilizador que a utiliza no momento em que se precisa que este esteja autorizado.

Actividades de Aprendizagem

Actividade 1.1 - Definição e exemplos dos principios de segurança informática

Introdução

A evolução e a redução do custo de aquisição do computador, tornou mais atraente a possibilidade de utilização destes quer em ambientes isolados ou em ambientes em rede. Esta possibilidade de conexão de computadores em redes trouxe consigo algumas vantagens e também desvantagens.

Nesta actividade iremos discutir os conceitos básicos da segurança informática.

Detalhes da actividade

Para a realização desta actividade é importante que leia o texto a seguir:

Um sistema informático é dito seguro se responde a quatro requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade (incluí hardware, software, recursos e utilizadores).

Esta definição traz á tona os três objectivos básicos da segurança informática que são:

Confidencialidade: garantir restrições de acesso e divulgação da informação.

Integridade: Integridade é a "propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental".

Disponibilidade: é a propriedade de que a informação não esteja disponível a quem não tem autorização nem esteja credenciado.

A perda de uma dessas propriedades, terá como resultado os seguintes factores:

Perda de confidencialidade: A divulgação não autorizada de informação.

Perda de Integridade: A modificação não autorizada ou destruição de informações.

Perda de Disponibilidade: Rompimento de acesso ou uso da informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade, representa os principais atributos que, actualmente, orientam a análise, o planeamento e a implementação da segurança informática. Outros atributos importantes são o controle e auditoria.

Auditoria: Da mesma forma que um controle deve ser feito para evitar o acesso não autorizado a um sistema, deve ser feito também o controle de acções de utilizadores autorizados. Controles de auditoria devem permitir a criação de históricos de acessos válidos para, uma eventual verificação de actividades irregulares executadas por utilizadores devidamente autorizados.

Conclusão

Esta actividade introduziu os conceitos fundamentais de segurança informática.

Avaliação

Verifique a sua compreensão!

Os principais atributos que orientam a análise, o planeamento e a segurança para um grupo de informações que se deseja proteger são:

(A) Confidencialidade, Integridade, Disponibilidade.

(B) Confidencialidade, Persistência, Disponibilidade.

(C) Confidencialidade, Integridade, Durabilidade.

(D) Consistência, Integridade, Disponibilidade.

(E) Confiabilidade, Integridade, Disponibilidade.

Qual dos princípios básicos da segurança da informação enuncia a garantia de que uma informação não foi alterada durante seu percurso, da origem ao destino?

(A) Não-repúdio

(B) Integridade

(C) Autenticidade

(D) Disponibilidade

(E) Confidencialidade

Actividade 1.2 - [Desafios da seguraça informática]

Introdução

As tecnologias da informação e comunicação são hoje meios indispensáveis em qualquer actividade da sociedade. Ameaças contra a sua disponibilidade, integridade e confidencialidade podem resultar em ocorrências nefastas para o normal decurso das actividade das instituições.

A segurança informática é também um tópico que tem vindo a merecer bastante atenção, por parte dos profissionais de TI em particulae e no geral pela sociedade.

Detalhes da atividade

Alguns dos desafios de segurança de computadores são:

Complexidade: A segurança informática pode parecer para ser fácil de implementar, porque suas exigências são simples, temos confidencialidade, autenticação, não repúdio, integridade. Mas os mecanismos utilizados para atender a esses requisitos podem ser bastante complexos, e compreendê-los pode envolver raciocínio bastante sutil;

Desenvolvimento e posse dos algoritmos de segurança: mecanismo de segurança pode exigir mais de um algoritmo ou protocolo; ele também pode exigir alguns indivíduos para manter alguma informação secreta (por exemplo, uma chave criptográfica). Isso traz um desafio de criação, distribuição e protecção dessas informações secretas. Também pode haver uma dependência de protocolos de comunicações, cujo comportamento pode complicar o processo de desenvolvimento do mecanismo de segurança;

Colocação de algoritmo de segurança: Se o seu algoritmo de segurança for bem sucedido, há um outro desafio que é saber onde usá-lo. Isso é necessário tanto para colocação física (por exemplo, em que pontos de uma rede são necessários certos mecanismos de segurança) e num sentido lógico (por exemplo, em que camada ou camadas de uma arquitetura, tais como TCP / IP deve ser o algoritmo de segurança colocado).

Possíveis ataques: Ao desenvolver um mecanismo de segurança específico ou algoritmo, deve-se sempre em primeiro lugar analisar os potenciais ataques sobre esses recursos de segurança. No entanto, os ataques bem-sucedidos são projetados por analisar o problema de uma forma completamente diferente;

Desafio de conhecimentos: A segurança do informática é normalmente uma batalha entre as mentes de uma pessoa que está tentando encontrar falhas de segurança e o administrador que tenta reduzí-las ou eliminá-las. A principal vantagem da pessoa tentando encontrar falhas de segurança é que ele ou ela só precisa encontrar uma única fraqueza, enquanto o administrador deve encontrar e eliminar todos os pontos fracos para alcançar a segurança perfeita;

Ignorância: Há uma tendência natural por parte de utilizadores do sistema e administradores a compreender a necessidade de investimento em segurança até que ocorra uma falha de segurança;

Falta de tempo: A segurança do computador precisa de constante monitoramento e isso às vezes é um grande desafio para algumas pessoas devido à falta de tempo devido a sobrecarga de tarefas.

Mau planeamento: Segurança de computador é na maioria das vezes incorporadas num sistema depois que o projeto estiver completo, em vez de ser uma parte integrante do processo de design. Às vezes, é visto também como um obstáculo ao funcionamento eficiente e de fácil utilização de um sistema de informação ou uso da informação.

Conclusão

Nesta lição abordamos os principais desafios encontrados aquando da impelmentação de políticas de segurança.

Avaliação da actividade

Avaliação

1. Até que ponto o mau planeamento pode influenciar negativamente na segurança da rede?

Actividade 1.3 - Modelo de segurança informática

Introdução

Nesta actividade iremos abordar o modelo de segurança informática, onde iremos fazer uma abordagem dos recursos de um sistema computacional assim como as vulnerabilidades a que estes estão expostos.

Detalhes da atividade

Modelo de Segurança informática

No modelo de segurança informática, precisamos de olhar para recursos do sistema, ou activo, que se desejam proteger. Pode listar os seguintes recursos do sistema:

Hardware: a parte física do computador, composta pelos diferentes dispositovos electónicos.

Software: É a parte lógica do computador . Esta é composta por conjuntos organizados de instruções para operar o sistema computacional.

Dados: Dados consiste de fatos brutos, que o computador pode manipular e transformar em informação que é útil para as pessoas.

Instalações e redes de comunicações: as rede de de comunicação de dados e dispositivos de comunicação.

Utilizadores: Alguns tipos de computadores podem operar sem muita intervenção de pessoas, mas os computadores pessoais são projectados especificamente para serem usados por pessoas.

Nos termos de segurança informática, estes recursos do sistema podem estar sob diferentes categorias de vulnerabilidades. As categorias gerais de vulnerabilidades de um dos recursos de sistema de computador ou recursos de rede são:

Vulnerabilidades que correspondem à tríade CIA: Os recursos do sistema de computador podem ser corrompidos, para que ele execute acções não solicitadas. Por exemplo, valores de dados armazenados podem ser indevidamente modificados. Recursos do sistema computacional também podem se tornar permeáveis. Por exemplo, alguém que não deve ter acesso a algumas ou todas as informações disponíveis através na rede obtém tal acesso. Finalmente, eles podem se tornar indisponíveis ou muito lento. Ou seja, usando o sistema ou rede torna-se impossível.

Ameaças: Uma ameaça é o principal perigo de segurança para os recursos do computador. Eles são capazes de explorar as vulnerabilidades de segurança do computador. Um ataque é um tipo de ameaça que, se realizado com sucesso pode levar a uma violação indesejável de segurança do computador, ou consequência ameaça. As pessoas que executam este tipo de ataque são conhecidas como atacantes. Os ataques podem ser de dois tipos; ataque activo que é uma tentativa de alterar os recursos do sistema ou afetar seu funcionamento e ataque passivo que é uma tentativa de aprender ou fazer uso de informação do sistema que não afecta os recursos do sistema.

Estes tipos de ataques também podem ser classificados de acordo com a origem do ataque, ou seja, ataque interno que é iniciado por uma pessoa/item dentro do perímetro de segurança (um "insider") e ataque externo que é iniciado por uma pessoa/produto fora da perímetro, por um utilizador não autorizado ou ilegítimo do sistema (um "estranho").

Esses tipos de ataques podem ser controladas no âmbito do processo conhecido como contramedida. Trata-se de prevenção, onde um ataque em particular é impedido de ser executado com sucesso. Se a prevenção falhar, então o próximo passo é para detectar o ataque e, em seguida, recuperar dos efeitos do ataque.

Conclusão

Nesta lição discutimos o conceito de modelo de segurança informática onde vimos quais os recursos a proteger e as vulnerabilidades que estes estão expostos.

Avaliação da actividade

- A que tipo de vulnerabilidades estão expostos os recursos do sistema computacional?

Resumo da Unidade

Nesta lição foram abordados os seguintes assuntos:

Conceitos básicos da segurança informática, princípios de segurança, incluindo os objectivos principais da segurança informática;

Desafios da segurança informática;

O modelo de segurança do computador, bem como os activos importantes do computador e recursos que precisam ser protegidos.

Avaliação da Unidade

Verifique a sua compreensão!

Estratégia de avaliação

Nesta unidade foram aplicadas avaliações contínuas e sumativas.

A avaliação contínua foi composta por vários componentes, como resolução de

problemas, questionáriose e trabalhos.

A estratégia de avaliação destina-se a testar a:

conhecimento obtido em conceitos-chave de segurança informática

Capacidade de entender os diferentes desafios de segurança do computador

O exame é utilizado para avaliar o conhecimento geral do modelo de segurança do computador

Critérios de Avaliação:

Para a configuração exame e marcando os critérios de avaliação genéricos UVA será usado.

Para a atribuição, os critérios serão elaborados adequada às competências avaliadas, com base nos critérios de marcação genéricos UVA

Sistema de classificação

Consulte a Tabela de avaliação do curso acima

Comentários

Esta unidade deverá ser conduzida com recurso á:

Palestras interactivas;

Discusão em pares;

Tutoria, onde o aluno poderá esclarer todas as dúvidas;

Avaliação sumativa agendadas (relatório de laboratório e de trabalhos) devolvidos aos estudantes, com comentários.

Oportunidades de consulta ao tutor com recurso a ferramentas de comunicação síncronas e assíncronas (Presencial ou remotamente)

Questionário

Instruções

Responda com clareza as questões que lhe são colocadas.

1. Apresente o conceito de segurança informática.
2. Descreva detalhadamente os princípios de segurança.
3. O que significa perda de segurança?
4. Descreva detalhadamente os elementos que compõem o conjunto de recursos de um sistema computacional e do tipo de vulnerabilidades que estão expostos.

Soluções esperadas na unidade 1:

Avaliação da actividade 1.1

1. A
2. B

Avaliação da actividade 1.2

Palavras-chave

1. Vulnerabilidades na rede.

Avaliação da actividade 1.3

Palavras-chave

1. Confidencialidade, integridade e disponibilidade.

Avaliação da unidade

Palavras-chave

1. Protecção, acesso não autorizado e não repúdio.
2. Confidencialidade, integridade e disponibilidade.
3. Não verificação da tríade CIA.
4. Hardware, software, utilizadores

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 2. [Ataques, ameaças e vulnerabilidades no computador]

Introdução

Nesta unidade iremos discutir os diferentes tipos de ameaças e ataques. Ele também apresentar algumas vulnerabilidades que os sistemas computacionais estão expostos, bem como os mecanismos de prevenção diferentes.

Objetivos da Unidade

Após a conclusão desta unidade, você deverá ser capaz de:

Identificar os diferentes tipos de ameaças e ataques

Relacionar as ameaças e os activos de computador

Identificar as vulnerabilidades de segurança do computador

Ter noções de criptografia e suas implementações

Seleccionar os mecanismos de monitorização dos sistemas adequados ás vulnerabilidades do mesmo e seus modos de acção.

Termos-chave

Ameaças externas; Representam todos os ataques oriundos de fora do ambiente da Organização com o objectivo de explorar as vulnerabilidades de uma determinada rede para uma finalidade qualquer. Elas representam um alto grau de participação nas pesquisas sobre ataques a sistemas computacionais.

Ameaça Interna: Estão presentes no dia-a-dia das organizações, cada uma com o seu grau de periculosidade, podendo ser desde um procedimento inadequado de um funcionário, até uma acção internacional, com o intuito de interromper a execução de um processamento em determinado sistema.

Ameaça Incidental: Este tipo de ameaça é muitas vezes inerente às próprias condições de operacionalidade quotidiana.

Ataques passivos: ataques passivos têm a natureza de espionagem de, ou monitoramento de transmissões

Ameaça Intencional. Tanto se pode referir a uma intromissão não autorizada e com intenções de aproveitamento dos recursos informáticos com fins alheios à organização proprietária, como à possibilidade de serem perpetrados sofisticados ataques, com a utilização de amplos conhecimentos do sistema operativo;

Ameaça Passiva. Embora possa ser de natureza incidental ou intencional, não corresponde nem a nenhuma modificação da informação, nem à alteração dos recursos ou do funcionamento do sistema;

Ameaça Activa. Independentemente do seu nível, conduz a uma modificação da informação presente no sistema ou dos seus processos de funcionamento. Como exemplos, podemos indicar alterações de ficheiros, de caminhos, de directórios e de passwords.

Ataque ativo: ataques activos envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso

Ataques internos: este tipo de ataque acontece se os utilizadores legítimos de um dado sistema assumem comportamentos não autorizados ou não esperados.

Ataques externos: neste tipo de ataques, as técnicas utilizadas incluem a captação de dados, a intercepção de emissões, as masquerades e a mera ultrapassagem das fases de autenticação e/ou dos mecanismos de controle de acessos;

Criptografia – processo pelo qual uma mensagem (o texto limpo) é transformada em uma segunda mensagem (o texto cifrado) usando uma função complexa (o algoritmo de criptografia) e uma chave criptográfica especial;

Decifragem – o processo inverso, pelo qual o texto cifrado é transformado no texto limpo, usando-se uma função complexa e uma chave de decifragem. Em alguns sistemas criptográficos, a chave criptográfica e a chave de decifragem são iguais em outros, são diferentes.

Actividades de Aprendizagem

Actividade 1.1 - Ameaças e Ataques

Introdução

Para se garantir a protecção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para a protecção desses recursos. Neste tópico iremos apresentar as ameaças e ataques a que um sistema informático está exposto.

Detalhes da actividade

PAra a realização desta actividade deverá ler o texto que se segue:

Tipos de ameaças e ataques

Existem quatro tipos de ameaças e diferentes tipos de ataques que resultam como consequência das mesmas.

1. Disclosure: acesso não autorizado à informação

Esta é uma ameaça para um componente da tendência conhecida como CIA confidencialidade. Os seguintes tipos de ataques podem resultar em consequência desta ameaça:

Exposição: Isto pode ser intencional, onde alguém voluntariamente fornecer informações sensíveis, tais como números de cartão de crédito, a pessoa não autorizada. Ele também pode ser o resultado de um ser humano, hardware, software ou de erro, o que resulta na divulgação de dados sensíveis a pessoas não autorizadas.

Intercepção: Este tipo de ataque é comum em sistemas de comunicações, principalmente numa LAN. Os dispositivos conectados à rede local podem receber uma cópia dos pacotes destinados ao outro dispositivo. Na Internet, um hacker determinado pode ter acesso ao tráfego de e-mail e outras transferências de dados. Todas estas situações criam o potencial para o acesso não autorizado aos dados.

Inferência: Análise de tráfego é o principal tipo de ataque interferência. Ela envolve a obtenção de informações a partir da observação do padrão de tráfego em uma rede, como a quantidade de tráfego entre particulares dispositivos de comunicação na rede.

Intrusão: Trata-se de um atacante obter acesso não autorizado a dados sensíveis, ignorando as proteções de controle de acesso do sistema.

2. Deception: aceitação de dados falsos, indução ao erro.

Esta é uma ameaça para um componente da tríade CIA conhecida como integridade. Os seguintes tipos de ataques podem resultar em consequência desta ameaça:

Masquerade: Neste caso, há sempre uma entidade que pretende assumir o papel da outra, isto é, um utilizador não autorizado tenta fazer-se passar por um utilizador autorizado. Este tipo é usado com outras formas de ataque activas, o replay e a modificação de mensagens.

Falsificação: Esta é a capacidade de alterar ou substituir dados válidos ou colocar dados falsos num arquivo ou banco de dados. Por exemplo, um estudante pode alterar suas notas em um banco de dados da escola.

Repúdio: Neste caso, um utilizador nega o envio de dados ou a recepção ou a posse dos dados.

3. Disruption: interrupção ou prevenção da operação correta de um sistema Esta é uma ameaça para dois dos componentes da tríade CIA, disponibilidade e integridade. Os seguintes tipos de ataques podem resultar como consequência desta ameaça:

Incapacidade: Este é um ataque a disponibilidade do sistema. Isso pode acontecer como resultado da destruição física ou dano de hardware do sistema. Neste caso o Malware, o software malicioso, actua de modo a desactivar um sistema ou alguns dos seus serviços.

Corrupção: Este é um ataque à integridade do sistema. Um utilizador pode obter acesso não autorizado a um sistema e modificar algumas de suas funções.

Obstrução: Este tipo de ataque envolve a obstrução do funcionamento do sistema de tal forma que o utilizador pode ser capaz de interferir nas comunicações desabilitando vias de comunicação ou alterando informações de controle de comunicação. Envolve também a sobrecarga do sistema, colocando o excesso de carga sobre o tráfego de comunicação ou recursos de processamento.

4. Usurpação

Esta é uma ameaça para um dos componentes de tríade CIA conhecido como integridade. Os seguintes tipos de ataques podem resultar como consequência desta ameaça:

Misappropriation: Trata-se de roubo de serviço. Um exemplo é um ataque distribuído de negação de serviço (DDoS). Neste caso, o software malicioso faz uso não autorizado dos recursos do processador e sistema operativo.

Misuse: O uso indevido pode ocorrer por meio de qualquer software malicioso ou um hacker que ganhou o acesso não autorizado a um sistema. Em ambos os casos, as funções de segurança podem ser desativadas ou frustrado.

Conclusão

Nesta atividade foram apresentadas diferentes tipos de ameaças e os ataques que podem surgir como consequência delas.

Avaliação

Verifique a sua compreensão!

1. Qual dos principios de segurança fica comprometido com a ocorrência do ataque do tipo replay?

Actividade 1.2 - Ameaças e activos

Introdução

Nesta unidade, iremos discutir a relação entre ameças e activos num sistema computacional.

Detalhes da atividade

A segurança informática deve estar focalizada em quatro aspectos:

Aplicações;

Hardware;

Recursos;

Utilizador.

Nesta atividade, iremos abordar esses quatro aspectos e relacioná-los com os conceitos dos três componentes da tríade CIA.

HARDWARE: A principal ameaça para o hardware do sistema computacional é a ameaça a um dos componente da tríade CIA chamado de disponibilidade. O componente de um sistema de computador hardware é o mais vulnerável a ataques e menos suscetível a controles automatizados. As ameaças podem ser de diferentes tipos, tais como danos acidentais e/ou deliberados para diferentes dispositivos, bem como o seu roubo. Roubo de dispositivos de memória, pode levar à perda de confidencialidade que é onde a informação sensível é principalmente mantida. São necessárias medidas físicas e administrativas de segurança para lidar com essas ameaças.

SOFTWARE: Mais uma vez a principal ameaça para o software é um ataque à componente da tríade CIA chamado de disponibilidade. Os softwares de aplicação, podem ser facilmente apagados, alterados ou danificados. A gestão cuidadosa de configuração de software, inclui fazer cópias de segurança da versão mais recente do software, mantendo desse jeito uma alta disponibilidade.

Dados e utilizadores: A segurança dos dois componentes discutidos anteriormente (hardware e software) são uma preocupação para os profissionais de computação assim como para utilizadores domésticos. O principal problema é a segurança dos dados, que envolve arquivos e outros tipos de dados. As preocupações de segurança em relação aos dados são amplas, abrangendo a disponibilidade, confidencialidade e integridade. No caso de disponibilidade, a preocupação é com a destruição de dados, que pode ocorrer acidentalmente ou intencionalmente. A preocupação óbvia com o sigilo é o acesso não autorizado de dados, e esta área tem sido objecto de, talvez, mais pesquisa e esforço do que qualquer outra área da segurança informática. Finalmente, a integridade dos dados é uma preocupação importante na maioria das instalações. Modificações de dados pode ter consequências que variam de menor a desastrosa.

LINHAS E REDES DE COMUNICAÇÃO: ataques de segurança de rede podem ser classificados como ataque passivo e ataque ativo.

Ataques passivos: têm a natureza de espionagem de, ou monitorização de transmissões. O objetivo do atacante é a obtenção de informação que está sendo transmitida. Dois tipos de ataques passivos são:

A liberação do conteúdo da mensagem: A mensagem, como uma conversa telefônica, uma mensagem de correio electrónico ou um arquivo transferido podem conter informações sensíveis ou confidenciais e podem ser facilmente percebidas, de modo que o atacante pode ter acesso ao conteúdo desta mensagem. Isto é mostrado na Figura 2, abaixo.

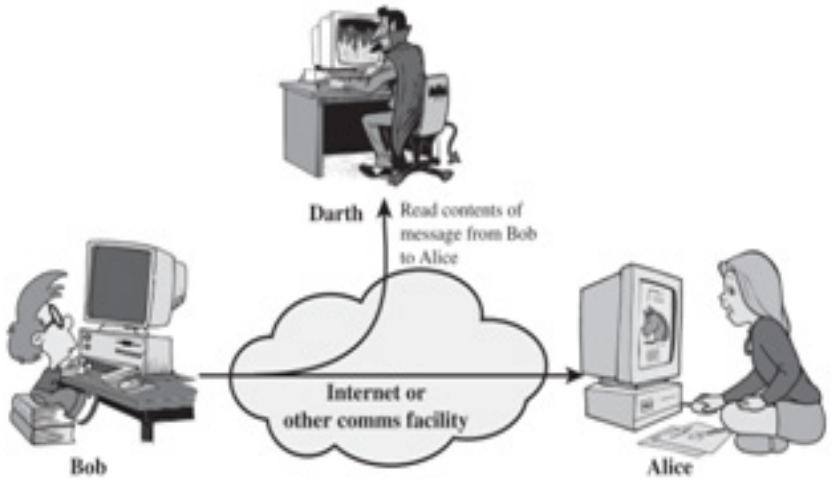

Figura 1: Mostrando a libertação de ataque conteúdo da mensagem

Análise de tráfego: Suponha que tivéssemos uma forma de mascarar o conteúdo de mensagens ou outro tráfego de informações para que os atacantes, mesmo capturando a mensagem, não poderia extrair as informações a partir da mensagem. A técnica comum para conteúdos de mascaramento é a criptografia. Mesmo com os dados criptografados, o atacante ainda pode ser capaz de observar o padrão dessas mensagens, e determinar a localização e a identidade dos hosts de comunicação e poderia observar a frequência e duração das mensagens trocadas. Esta informação pode ser útil na identificação da natureza da comunicação que estava ocorrendo.

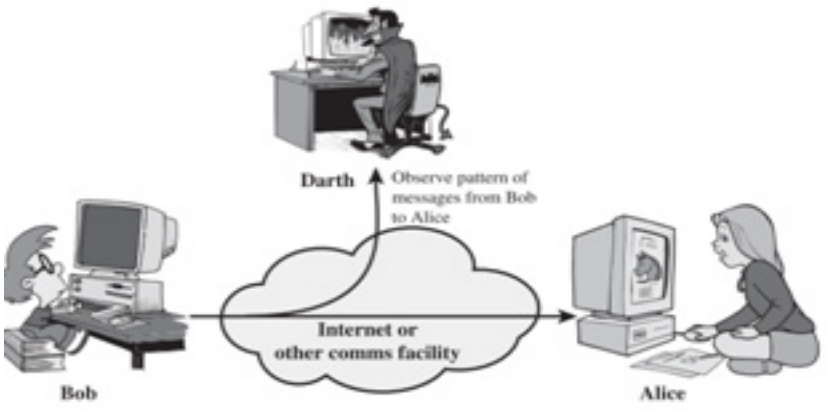

Figura 2: Mostrando ataque Análise de tráfego

Ataque activo: envolvem alguma modificação do fluxo de dados ou a criação de uma falsa corrente. Consiste quatro categorias:

Masquerade: Neste caso, há sempre uma entidade que pretende assumir o papel da outra, isto é, um utilizador não autorizado tenta fazer-se passar por um utilizador autorizado. Este tipo é usado com outras formas de ataque activas, tais como o replay e a modificação de mensagens.

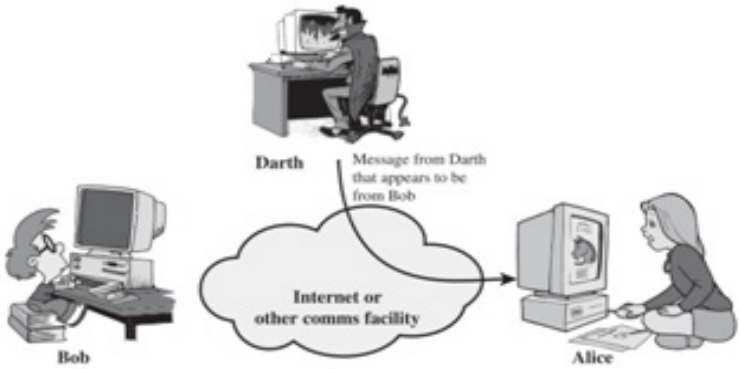

Figura 3: Mostrando ataque Masquerade

Replay: Este ataque acontece quando uma mensagem ou parte dela é reenviada para produzir um efeito que não estteja autorizado;

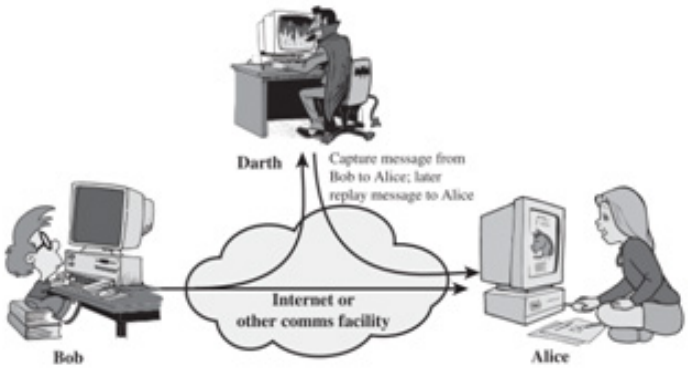

Figura 4: Ataque Reply

Modificação de mensagens :Tal ocorre quando o conteúdo de uma transmissão de dados é alterado, sem que essa alteração seja detectada.

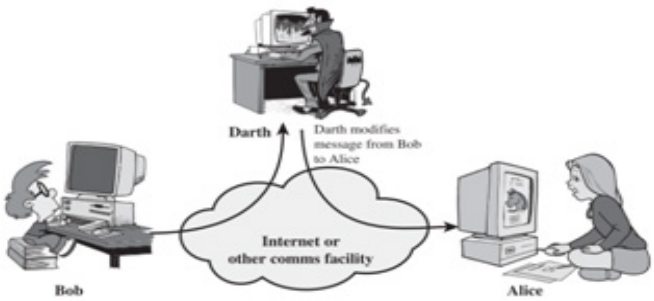

Figura 5: Ataque modificação de mensagens

Negação de Serviço (Denial of Service - DoS): A ideia deste ataque é fazer com que algo pare de funcionar. Segundo Strauch, S (1999), trata-se de um tipo de ataque, o qual inclui ataques como sobrecarga da rede, excessivos pedidos de abertura de conexão (Syn flooding), etc..

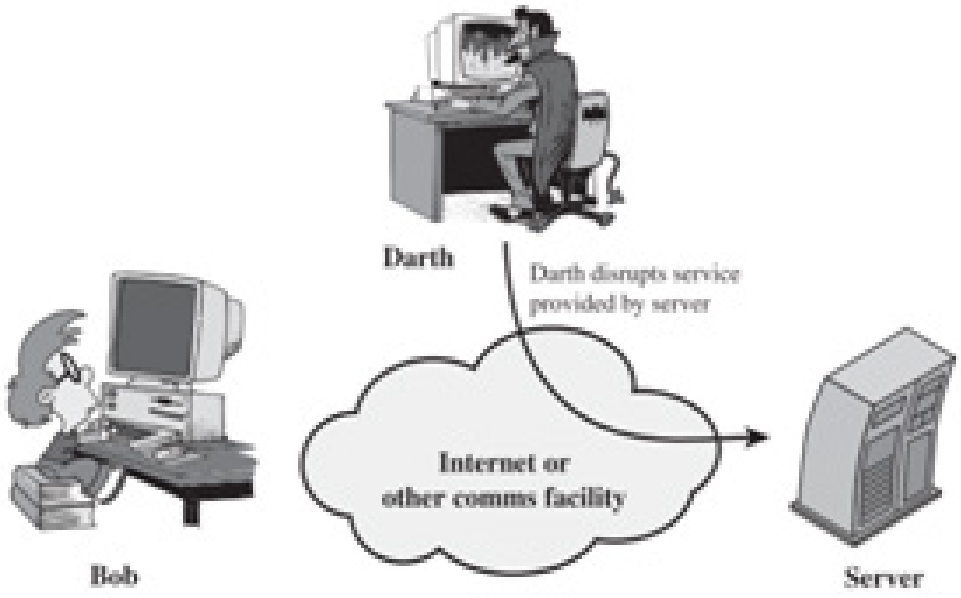

Figura 6: Ataque DoS

Conclusão

Esta actividade explicou a relação entre ameaças e ativos de computador.

Avaliação

1. Apresente a relação entre os activos de um sistema computacional e as possiveis ameaças.

Actividade 1.3 - Vulnerabilidades

Introdução

Num sistema computacional, podem-se considerar vulnerabilidades como falhas ou fraquezas que se exploradas, conduzem a uma perda ou fuga de alguma informação.

Nesta unidade iremos discutir as vulnerabilidades de um sistema computacional.

Detalhes da atividade

Uma vulnerabilidade pode partir das próprias medidas de segurança implantadas na organização, se existir estas medidas, porém configuradas de maneira incorreta, então a empresa possuirá uma vulnerabilidade e não uma medida de segurança.

As vulnerabilidades podem ser encontradas no modo de agir das pessoas, nos equipamentos, ou nos sistemas ou softwares. Conhecendo as vulnerabilidades que podem contribuir para a ocorrência de incidentes de segurança, fica facilitada a identificação de medidas preventivas.

Tipos de vulnerabilidades

As vulnerabilidades ou pontos fracos são citados da seguinte maneira:

1. Naturais: São aquelas que envolvem condições naturais, que podem trazer riscos para os equipamentos e as informações. Podemos citar: locais propensos a inundações, ambientes sem a devida proteção contra incêndio, terremotos, furacões ou maremotos.

2. Físicas: São ambientes com pontos fracos de ordem física, onde são armazenadas ou gerenciadas as informações. Estas situações podem comprometer a disponibilidade da informação. Tais como, instalações inadequadas para o trabalho, falta de extintores contra incêndio, locais desorganizados ou pessoas não-autorizadas transitando no local tirando a privacidade no manuseio das informações sigilosas.

3. Hardwares: Estão relacionadas aos equipamentos que apresentam defeitos de fabricação ou configuração, podendo permitir o ataque de vírus ou violações. Nestas situações encontram-se a falta de atualizações dos programas e equipamentos não dimensionados corretamente.

4. Softwares: São os pontos fracos existentes nos aplicativos permitindo o acesso de indivíduos não-autorizados. Por esta razão que os softwares, são os mais preferidos dos elementos que buscam as ameaças. Exemplo: Aplicativos com configurações ou instalações inadequadas, programas de e-mail que permitem a execução de códigos maliciosos e falta de atualizações.

5. Armazenamento: As informações são armazenadas em suportes físicos (disco rígido) ou magnéticos (CD, DVD, Cartão de memória, Pen drive, fitas magnéticas.....).Suas utilizações inadequadas podem ocasionar uma vulnerabilidade, afetando a integridade, a disponibilidade e a confidencialidade das informações. Os pontos fracos podem danificar ou indisponibilizar os meios de armazenamento. Exemplo: defeito de fabricação, uso incorreto, prazo de validade e expiração.

6. Comunicação: Está relacionado com o tráfego de informações. Estes tráfegos podem ser realizados através de fibra óptica, ondas de rádio, satélite ou cabos. O sistema de comunicação escolhido deve ser seguro de modo que as informações transmitidas alcancem o destino desejado e que não sofra nenhuma intervenção alheia. As informações deverão ser criptografadas e após alguma falha no processo a informação não deverá ficar disponível para pessoas não-autorizadas e muito menos perder sua confiabilidade.

7. Humanas: Podem ser de atitudes intencionais ou não, os pontos fracos são: uso de senha fraca, compartilhamento de credencial de acesso, falta de treinamentos para o utilizador, a não consciência ou desconhecimento de segurança da informação e funcionários descontentes.

As principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos utilizadores que, inadvertidamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis ou mesmo contaminam seus arquivos e programas com vírus de computadores.

A exploração de uma vulnerabilidade, por um indivíduo mal intencionado ou não, num sistema informático leva a efectivação de um ataque ao sistema.

Conclusão

Nesta lição foram discutidas as diferentes vulnerabilidades de segurança informática.

Avaliação

1. Fazendo a análise dos tipos de vulnerabilidade acima discutidos, em caso de efectivação de um ataque quais os princípios de segurança ficam comprometidos.
2. Que tipo de ameaças estão ligadas a cada uma das vulnerabilidades acima apresentadas.

Actividade 1.4 - Criptografia

Introdução

A partilha de informações sigilosas é uma necessidade antiga. Com o surgimento da internet e de sua consequente facilidade de transmitir dados de maneira precisa e extremamente rápida, a criptografia tornou-se uma ferramenta fundamental para permitir que apenas o emissor e o receptor tenham acesso à uma determinada informação. Esta lição tem como objetivo fazer uma abordagem introdutória à criptografia, mostrando os aspectos e conceitos mais importantes.

Detalhes da actividade

A confidencialidade e privacidade são quesitos importantes quando o assunto é segurança. Entretanto, hackers podem roubar informação que é considerada crítica para uma pessoa ou uma organização.

As redes de comunicação normalmente são inseguras, submetendo a informação que trafega a ameaças passivas e activas.

Uma forma de proteger esta informação contra ameaças passivas e/ou ativas chama-se criptografia.

Criptografia – processo pelo qual uma mensagem (o texto limpo) é transformada em uma segunda mensagem (o texto cifrado) usando uma função complexa (o algoritmo de criptografia) e uma chave criptográfica especial;

Decifragem – o processo inverso, pelo qual o texto cifrado é transformado no texto limpo, usando-se uma função complexa e uma chave de decifragem. Em alguns sistemas criptográficos, a chave criptográfica e a chave de decifragem são iguais em outros, são diferentes.

A criptografia é usada para prover serviços como autenticação e integridade.

Nas mensagens de e-mail, por exemplo, a criptografia pode fornecer:

Autenticação – permite ao destinatário da mensagem validar sua origem. Isto preveniria que um impostor mentisse que era o remetente da mensagem;

Integridade – assegura ao destinatário que a mensagem não foi modificada ao longo da rota. Observa-se que a integridade permite ao destinatário detectar modificação da mensagem, mas não impedí-la.

Confidencialidade – previne a não revelação da mensagem para quem não está autorizado.

Não-repudiação – recibos criptografados são criados, de forma que o autor de uma mensagem não possa negar falsamente que a tenha enviado.

A criptografia pode ser feita segundo dois métodos básicos:

Criptografia com Chaves Secretas (ou Simétricos)

Este método de criptografia, consiste em substituir as letras de uma mensagem pela n-ésima letras após a sua posição no alfabeto. Assim o texto criptografado produzido para um mesmo texto normal pode variar de acordo com o valor de n, que é a chave utilizada nos processos de codificação e decodificação do método.

Criptografia com Chave Pública (Assimétricos)

Este método de criptografia baseia-se na utilização de chaves distintas: uma para codificação (E) e outra para a decodificação (D), escolhidas de forma que a derivação de D a partir de E seja em termos práticos, senão impossível, pelo menos difícil de ser realizada.

Conclusão

Nesta lição discutimos o mecanismo de segurança chado criptografia.

Avaliação

Responda as questões que se seguem com clareza.

- Que principio de segurança é garantido com a implementação da criptografia?
- Diferencie a criptografia simétrica da assimétrica.

Actividade 1.5 -Assinatura digital

Introdução

Neata lição iremos discutir omecanismo de assinatura digital.

Detalhes da actividade

Pode-se definir a assinatura digital como o conjunto de dados que se associam a uma unidade de dados para protegê-los contra a falsificação, permitindo ao receptor comprovar a fonte e a integridade dos mesmos. Dado que utilizam tecnologias de encriptação muito poderosas, as assinaturas digitais apresentam uma grande segurança, até maior do que as assinaturas reais, pois estas podem ser falsificadas.

A utilização da assinatura digital providencia a prova de que uma mensagem veio do emissor. Para verificar este requisito, uma assinatura digital deve ter as seguintes propriedades:

Autenticidade - o receptor deve poder confirmar que a assinatura foi feita pelo emissor;

Integridade - qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;

Não-repúdio - o emissor não pode negar a autenticidade da mensagem.

Existem diversos métodos para assinar digitalmente documentos, e esses métodos estão em constante evolução. Porém de maneira resumida uma assinatura típica envolve dois processos criptográficos: o hash (resumo) e a encriptação deste hash.

Em um primeiro momento é gerado um resumo criptográfico da mensagem através de algoritmos complexos que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho. A este resumo criptográfico se dá o nome de hash. Uma função de hash deve apresentar necessariamente as seguintes características:

Deve ser impossível encontrar a mensagem original a partir do hash da mensagem.

O hash deve parecer aleatório, mesmo que o algoritmo seja conhecido. Uma função de hash é dita forte se a mudança de um bit na mensagem original resulta em um novo hash totalmente diferente.

Deve ser impossível encontrar duas mensagens diferentes que levam a um mesmo hash.

Neste ponto, o leitor mais atento percebe um problema: Se as mensagens possíveis são infinitas, mas o tamanho do hash é fixo, é impossível impedir que mensagens diferentes levem a um mesmo hash. De fato, isto ocorre. Quando se encontram mensagens diferentes com hashs iguais, é dito que foi encontrada uma colisão de hashes. Um algoritmo onde isso foi obtido deve ser abandonado.

As funções de hash estão em constante evolução para evitar que colisões sejam obtidas. Cabe destacar porém que a colisão mais simples de encontrar é uma aleatória, ou seja, obter colisões com duas mensagens geradas aleatoriamente, sem significado real. Quando isto ocorre os estudiosos de criptografia já ficam atentos, porém para comprometer de maneira imediata a assinatura digital seria necessário obter uma mensagem adulterada que tenha o mesmo hash de uma mensagem original fixa, o que é teoricamente impossível de ocorrer com os algoritmos existentes hoje. Desta forma, garante-se a integridade da assinatura.

Após gerar o hash, ele deve ser criptografado através de um sistema de chave pública para garantir a autenticação e a irretratabilidade. O autor da mensagem deve usar sua chave privada para assinar a mensagem e armazenar o hash criptografado junto a mensagem original.

Para verificar a autenticidade do documento, deve ser gerado um novo resumo a partir da mensagem que está armazenada, e este novo resumo deve ser comparado com a assinatura digital. Para isso, é necessário descriptografar a assinatura obtendo o hash original.

Conclusão

Nesta lição discutimos a criptografia por assinatura digita, bem como o seu funcionamento.

Avaliação

1. Quais princípios da segurança da informação são obtidos com o uso da assinatura digital?

   (A) Autenticidade, confidencialidade e disponibilidade.

   (B) Autenticidade, confidencialidade e integridade.

   (C) Autenticidade, integridade e não-repúdio.

   (D) Autenticidade, confidencialidade, disponibilidade, integridade e não-repúdio.

   (E) Confidencialidade, disponibilidade, integridade e nãorepúdio.

Actividade 1.6 - Auditoria Informática

Introdução

Da mesma forma que um controle deve ser feito para evitar o acesso nãoautorizado a um sistema, deve ser feito também o controle de acções de utilizadores autorizados. Controles de auditoria devem permitir a criação de históricos de acessos válidos para, uma eventual verificação de actividades irregulares executadas por utilizadores devidamente autorizados.

Através da correcta aplicação desses princípios, a segurança informática pode trazer benefícios como: aumentar a produtividade dos utilizadores através de um ambiente mais organizado, maior controle sobre os recursos informáticos e, finalmente garantir a funcionalidade das aplicações críticas da organização.

Numa operação de auditoria são realizadas as seguintes actividades:

- Análise de risco
- avaliação do desempenho de um sistema
- Análise de danos causados por um ataque, falha ou simplesmente um
- desastre.

Detalhes da atividade

Riscos

Um risco existe quando uma ameaça, com potencial para causar algum dano, apresenta alto índice de probabilidade de ocorrência no ambiente computacional e um baixo nível de proteção.

O primeiro passo para desenhar uma política de segurança, consiste em responder as seguintes perguntas:

- que se pretende proteger?
- Contra o quê ou quem proteger?
- Quanto tempo, esforço, recursos e dinheiro se deve dispender para a obtenção de uma protecção adequada?

Estas questões, constituem parte fundamental de todo o processo de implementação de uma política de segurança, pois não se pode proteger sem conhecer os riscos que se correm, bem como a proveniência dos mesmos.

Análise de Riscos

A análise de risco consiste num processo de identificação e avaliação dos factores de risco presentes e de forma antecipada no ambiente organizacional, possibilitando uma visão do impacto negativo causado á organização. Através da aplicação desse processo, é possível determinar as prioridades de acção em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização (Moreira, 2001).

Segundo Moreira (2001), o processo de análise de risco deve, no mínimo, proporcionar as seguintes informações:

- Pontos vulneráveis do ambiente;
- Incidentes de segurança causado pela acção de cada ameaça;

Medidas de protecção adequadas para impedir ou diminuir o impacto de cada incidente.

A análise de risco fornece as directrizes para a identificação das medidas de segurança necessárias paara que o ambiente computacional duma determinada organização possa atingir o nível de segurança desejado.

A avaliação do desempenho de um sistema

Esta atividade faz parte de uma auditoria para medir a capacidade dos recursos de uma empresa e avaliar a capacidade efetivamente utilizada. Pode, então, propor mecanismos para otimizar a capacidade de atingir os objetivos da empresa fixou.

A monitorização e avaliação da implementação de regras e procedimentos.

Em qualquer negócio, deve haver um manual de procedimentos que definem a operação do negócio. Este é geralmente o departamento de TI dentro de uma empresa que está desenvolvendo um manual de procedimentos sobre ele. E neste manual o aspecto da segurança não é deixado de fora. Durante uma auditoria de segurança, o auditor irá verificar se o seu funcionamento o departamento de TI seguindo os procedimentos estabelecidos no manual de procedimentos

Análise dos danos

Esta atividade é geralmente realizada após o início de um ataque ou desastre que as perdas dentro de uma empresa. Ele vai avaliar os danos e impactos. Ele também pode propor um plano de recuperação.

Avaliar um período de mudança ou migração

Quando uma empresa está em processo de migração de um sistema para outro, ele pode patrocinar uma operação de auditoria que avaliará novo status componentes de funcionamento, ver se eles atendem as especificações definidas no momento do comando. Ele pode, então, propor melhorias ou simplesmente para oferecer a sua substituição total. Um processo de auditoria pode ser considerado o lançamento de um sistema. Ele também pode ser realizada em um determinado calendário. Em caso de ataques ou o fracasso de um sistema também pode executar uma auditoria de emergência. Para avaliar a segurança de um sistema durante uma auditoria de segurança, precisamos reconhecido e ferramentas padronizadas. Na próxima seção, vamos ver essas duas ferramentas.

A norma TCSEC

TCSEC – Trusted Computing System Evaluation Criteria (DOD, 85), também conhecido como Orange Book, para a avaliação de segurança de dispositivos de segurança (criptografia, firewalls, etc.). Com relação a software, o foco do TCSEC (DOD, 85) consistia na definição dos requisitos de segurança necessários para a garantia da confidencialidade das informações.

Em relação aos programas informáticos, a norma TCSEC definia os requisitos de segurança necessários para a garantia da confidencialidade das informações.

A norma ITSEC

Em 1991, uma comissão europeia conjunta da Alemanha, França, Holanda e Reino Unido publicou uma norma europeia para certificação de segurança intitulada ITSEC(Information Technologie Security Evaluation Criteria), baseada no TCSEC (DOD, 85), tornando-se depois um padrão europeu voltado tanto para a avaliação de produtos como de sistemas.

A norma europeia distingue-se da norte-americana, essencialmente, por separar a funcionalidade de segurança da garantia de segurança.

Conclusão

Nesta lição abordamos o mecanismo de segurança informática denominado auditoria informática.

Avaliação

- Em que consiste a auditoria informática (Auditoria de Segurança)?
- Quais o benefícios do conhecimento dos riscos por um administrador de sistemas?

Actividade 1.7 - [Monitorização]

Introdução

Os sistemas informáticos têm um papel cada vez mais importante numa instituição. A sua complexidade requer uma monitorização constante de equipamentos de hardware, software e comunicação, de forma a garantir um sistema fiável, robusto e de alta produtividade. Os resultados dessa monitorização são informação imprescindível para qualquer responsável pela administração de sistemas informáticos. No entanto, é cada vez mais comum disponibilizar parte dessa informação ao utilizador final, de modo a que este tenha uma melhor percepção do estado dos serviços que utiliza.

Detalhes da actividade

A monitorização de um sistema computacional, pode ser dividida em três grandes famílias:

Monitorização do sistema: Localizado no coração do sistema, que irá fornecer informações sobre o uso da CPU, memória.

Monitorização da rede: consiste em diagnosticar a disponibilidade do equipamento ligado a uma rede. As tecnologias utilizadas para este tipo de supervisão são bastante simples e o nível de informações retornadas é limitado.

Monitorização de aplicativos: graças a este acompanhamento, não teremos em conta apenas osequipamentos, mas também as aplicações que são executadas e as informações que eles retornam.

Conclusão

Nesta lição discutimos o mecanismo de monitorização de um sistema informático, bem como as componentes a monitorar.

Avaliação

- Que decisoões podemos tomar com os resultados da monitorização do sistema?

Soluções esperadas na unidade 2:

Avaliação da actividade 1.1

1. Integridade

Avaliação da actividade 1.2

Palavras-chave

1. Tríade CIA.

Avaliação da actividade 1.3

Palavras-chave

1. Confidencialidade, integridade e disponibilidade;
2. Ameaças passivas e ameaças passivas.

Avaliação da actividade 1.4

Palavras-chave

1. Confidencialidade;
2. As chave usada para cifrar e decifrar.

Avaliação da actividade 1.5

1. B

Avaliação da actividade 1.6

Palavras-chave

1. Análise deriscos, desempenho e danos ora causados;
2. Medidas de protecção.

Avaliação da actividade 1.7

Palavras-chave

1. Medidas de prevenção;

Resumo da Unidade

Nesta unidade, abordamos os conceitos de ameaças, ataques e vulnerabilidades, bem como os mecanismos para a redução ou mitigação dos mesmos.

Nesta abordagem foram destacados os seguintes tópicos:

- Ameaças e tipos de ataques;
- Ameaças e Ativos;
- Vulnerabilidades e ameaças;
- A criptografia;
- A criptografia e assinatura ao nível da aplicação Caso SSL;
- A criptografia e assinatura ao nível da rede: caso IPSec;
- Auditoria de segurança;
- Monitorização de um sistema informático.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 3. [Software Malicioso]

Introdução à Unidade

Esta unidade centra-se no estudo de softwares maliciosos e os seus métodos de mitigação.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

Identificar os diferentes tipos de software malicioso;

Mitigar a acção desses malwares.

Termos-chave

Malware: O termo malware é proveniente do inglês malicious software; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).

Vírus. São programas espúrios inseridos em computadores contra vontade de utilizador e desempenham funções indesejadas.

Worms. São Trojans ou vírus que fazem cópias do seu próprio código e as enviam para outros computadores, seja por e-mail, programas, dentre outras formas de propagação pela rede.

Actividades de Aprendizagem

Actividade 1.1 - Malware

Introdução

As maiores ameaças aos utilizadores de computadores quer conectados á Internet ou não, são representadas pelos Malwares.

Detalhes da actividade

Tipos de Malware

Vírus. São programas espúrios inseridos em computadores contra vontade de utilizador e desempenham funções indesejadas. Alguns vírus têm a capacidade de se reproduzir e infectar outros dispositivos por toda a rede. A cada dia surgem centenas de vírus e o combate a esse tipo de invasão é constante;

Fases de um vírus de computador:

Durante sua vida, um vírus típico atravessa as seguintes fases:

Fase dormente: o vírus é inactivo. O vírus irá eventualmente ser activado por evento, tal como uma data, a presença de outro programa ou arquivo. Nem todos os vírus passam por esta fase.

Fase de propagação: O vírus coloca uma cópia de si mesmo em outros programas ou em certas áreas do sistema no disco. A cópia pode não ser idêntica à versão propagação; vírus muitas vezes se transformar para evitar a detecção. Cada programa infectado irá agora conter um clone do vírus, iniciando deste modo a propagação.

Fase de Activação: O vírus é activado para realizar a função para a qual ele foi destinado. Como com a fase latente, a fase de desencadeamento pode ser causada por uma variedade de eventos do sistema, incluindo a contagem do número de vezes que esta cópia do vírus fez cópias de si mesmo.

Fase de execução: A função é executada. A função pode ser inofensiva, tal como uma mensagem no ecrã, ou prejudiciais, tais como a destruição de programas e arquivos de dados.

Mitigação de ataque de vírus

Esses tipos de aplicativos podem ser contidos através do uso eficaz de software antivírus e, potencialmente, ao nível da rede. O software antivírus pode detectar a maioria dos vírus e impedir a sua propagação na rede. Manter-se actualizado pode levar a uma postura mais eficaz contra esses ataques. Como novos vírus são liberados, as empresas precisam se manter atualizado com as últimas versões de software antivírus e aplicativos.

Trojans – Cavalos de Tróia. Os cavalos de Tróia são programas projectados para assumir controle de um servidor ou estação de trabalho de maneira furtiva, sem que o aministrador da rede ou o utilizador se dê conta.

Como exemplo, pode-se referir a possibilidade de enviar cópias de documentos sigilosos para os devidos utilizadores, mas também para um utilizador não autorizado a recebê-las.

Worms. São Trojans ou vírus que fazem cópias do seu próprio código e as enviam para outros computadores, seja por e-mail, programas, dentre outras formas de propagação pela rede. Eles têm se tornado cada vez mais comuns e perigosos porque o seu poder de propagação é muito grande.

Adware (Advertising software) é um tipo de software especificamente projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador. Em muitos casos, os adwares têm sido incorporados a softwares e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos. Um exemplo do uso legítimo de adwares pode ser observado na versão gratuita do browser Opera.

Spyware é o termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Existem adwares que também são considerados um tipo de spyware, pois são projectados para monitorar os hábitos do utilizador durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Existem ferramentas específicas, disponíveis na maioria dos distribuidores de antivírus, conhecidas como "anti-spyware", capazes de detectar e remover uma grande quantidade de programas spyware. Algumas destas ferramentas são gratuitas para uso pessoal e podem ser obtidas pela Internet.

Spam é o termo usado para se referir às mensagens eletrônicas não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é referenciada como UCE (do inglês Unsolicited Commercial E-mail).

Keylogger: Software que registra toda a atividade do teclado em um arquivo, que pode ser enviado para um provável atacante. Alguns Keyloggers são espertos o suficiente para registrar apenas as informações digitadas quando o utilizador conecta com um site seguro. Por amostrar as teclas que estão sendo digitadas, o Keylogger pode capturar números de contas, senhas e outras informações, antes delas serem processadas (criptografadas) por dispositivos de segurança.

Conclusão

Nesta lição discutimos o conceito de software malicioso, onde foram apresentados alguns tipos, bem como as técnica de mitigação dos mais comuns.

Avaliação

- Que cuidados devemos ter para que um antivírus funcione eficazmente?

Resumo da Unidade

Nesta unidade foram discutidos os softwares malicios, o seu funcionamento e bem como os cuidados a ter em cada um dos casos e as técnicas de mitigação dos mesmos.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

Critérios de Avaliação

Avaliação

Liste três tipos de software malicioso e apresente os métodos de

mitigação de cada um deles.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 4. Serviços de segurança

Introdução à Unidade

Nesta unidade temática, iremos introduzir alguns serviços de seguranca, tais como autenticação e controlo de acesso. Ainda nesta unidade iremos discutir alguns mecanismos de segurança tais como firewalls e mecanismos de detecção de intrusão.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Distinguir os diferentes meios de autenticação de utilizadores;
- Indicar os princípios dos métodos de controle de acesso;
- Descrever o funcionamento do mecanismo de controle de acesso;
- Identificar as bases de segurança e princípios de funcionamento de um sistema de detecção de intrusão e firewalls.

Termos-chave

Os serviços de segurança estão normalmente disponíveis em todos os sistemas operativos interligados em rede. Fazem parte dos serviços de segurança os seguintes:

Autenticação. Este serviço permite identificar, de forma inequívoca, as entidades que se encontram em contacto, isto é, entre as quais pode haver um fluxo de informação;

Integridade dos dados. Este serviço dá protecção contra ameaças activas, incluindo integridade de conexão com e sem recuperação, integridade de conexão com e sem recuperação, integridade de conexão por níveis e integridade dos níveis de conexão;

Confidencialidade de dados. Este serviço faculta a protecção de dados pessoais contra divulgações não autorizadas;

Não-recusa da origem. É necessário que o receptor tenha a possibilidade de obter certeza sobre a origem de mensagens e transacções;

Actividades de Aprendizagem

Actividade 1.1 - Autenticação

Introdução

Nesta atividade, serão discutidos diferentes métodos de autenticação de utilizadores.

Detalhes da actividade

Visão geral de autenticação

A autenticação do utilizador é a primeira linha de defesa num sistema computacional. Destina-se a evitar o acesso não autorizado a uma rede. É a base de definir controles de acesso. Ele é utilizado para fornecer a responsabilidade do utilizador.

Verificar a identidade do utilizador

A autenticação do utilizador tem duas etapas: identificação - apresentando o utilizador para o sistema de segurança. Identificação é o meio pelo qual um utilizador pretende ser uma identidade específica. Verificação - fornecer informações que se liga a entidade à identidade. Verificação é o método usado para provar que a alegação.

Meios de Autenticação

Existem diferentes meios de autenticação do utilizador:

Algo que o indivíduo sabe, e.g. senha, PIN;

Algo que o indivíduo possui (tokens), por exemplo, chave criptográfica, smartcard;

Algo que o indivíduo é, por exemplo, impressão digital, retina;

Algo que o indivíduo faz, e.g. padrão de escrita, padrão de fala

Autenticação por senha

A autenticação por senha é o meio mais comum de autenticação. Não requer nenhum hardware especial. O utilizador fornece um nome de utilizador e senha, em seguida, o sistema procura o nome de utilizador na base de dados, ele verifica se o par nome de utilizador e senha existe e, finalmente, fornece acesso ao sistema para o utilizador.

Ataques a autenticação baseada em senha:

Espionagem, que pode ser soluccionada com a criptografia;

Ataque de dicionário: Um ataque directo á base de dados de armazenamento de senhas pode ser usado para descobrir ou alterar senhas. Normalmente controles de acesso são aplicadas para proteger as bases de dados que armazenam arquivos de senha. No entanto, alguns hackers podem contornar essas medidas de controle e aceder os arquivos de senha.

Ataque a uma conta específica: O hacker pode estar determinado em adivinhar uma senha de uma conta específica até que descubra a senha correta para essa conta específica. O melhor método de evitar isso é através da aplicação do mecanismo de bloqueio de conta. Isso irá desativar a conta depois de um número de tentativas de login.

Sequestro de sessão ou estação de trabalho: o atacante pode monitorar quando a estação de trabalho não está sendo usado ou um hacker pode desligar a sessão do utilizador e eles se conectar. O principal mecanismo de prevenção é fazer logon automaticamente à estação de trabalho após um período de inactividade. Sistemas de detecção de intrusão podem ser usados para detectar alterações no comportamento do utilizador.

Exploração de erros do utilizador: Alguns sistemas fornecem senhas para os utilizadors. Estes tipos de senhas são muito difíceis de lembrar, o que leva os utilizadors a escrevê-las em algum lugar. Mecanismos de prevenção incluem treinamento de utilizadores, detecção de intrusão e senhas simples combinados com um outro mecanismo de autenticação.

Exploração de uso múltiplo de senha: Alguns utilizadores usam a mesma senha para diferentes dispositivos, portanto, uma vez que o atacante descubra a senha, todos os dispositivos podem ser facilmente atacados.

Força da senha

Os utilizadors tendem a escolher senhas fracas se permitido. Esses tipos de senhas podem ser facilmente violadas via ataque de dicionário. Os utilizadores devem ser forçados a criar senhas mais complexas.

Autenticação baseada em tokens

Objectos que um utilizador dispõe para efeitos de autenticação do utilizador são chamados de fichas. Existem principalmente dois tipos de sinais que são largamente utilizados; estes são os cartões que têm a aparência e tamanho de cartões.

Eles são difíceis de duplicar e são facilmente transferíveis.

Exemplos de smartcard

Cartões de Banco / ATM

Cartões de crédito

Cartões de Viagem

Cartões acesso a um local de trabalho

Autenticação Biométrica

Autenticação baseada em dados biométricos é a utilização de características fisiológicas particulares dos utilizadores. Estes características são de diferentes tipos, tais como; Voz, Olho, impressão digital, etc. Comparado com senhas e tokens, a autenticação biométrica é tecnicamente complexa e cara.

Características Físicas usado em aplicações biométricas

As características físicas mais comuns usados na autenticação biométrica com base são os seguintes:

Características faciais: Este é um dos meios mais comuns para identificações de humanos. Baseia-se em algumas características-chave, tais como localização relativa e forma de características faciais chave, tais como olhos, sobrancelhas, nariz, lábios, e forma do queixo.

Impressões digitais: Uma impressão digital é o padrão de nervuras e sulcos na superfície da ponta do dedo. Este método é acreditado para ser único em toda a população humana.

A geometria da mão: Este método envolve a geometria da mão, isto é, sistemas de identificar as características da mão, tais como; forma, e comprimentos e larguras de dedos.

Padrão de retina: Acredita-se que o padrão formado pelas veias abaixo da superfície da retina é único e, por conseguinte, adequado para a identificação.

Voz: Este é um outro meio de identificação onde os padrões de voz são mais estreitamente ligada às características físicas e anatômicas do utilizador.

Operação de um sistema de autenticação biométrica

Para ser um utilizador autorizado, primeiro você deve estar inscrito na base de dados de utilizadores autorizados. Isto é semelhante a atribuir uma senha para um ID de utilizador específico. Com relação ao sistema biométrico, o utilizador dá o nome e senha ou PIN para o sistema. Ao mesmo tempo, o sistema detecta algumas características biométricas para isto é utilizador tais como, Iris, impressões digitais, etc. Todas estas entradas são digitalizados e o sistema extrai um conjunto de características que podem ser armazenados como um número ou um conjunto de números que representam esta característica biométrica única;

Dependendo da aplicação, a autenticação do utilizador num sistema biométrico envolve dois métodos:

Verificação: Este método é semelhante a um utilizador fazendo logon num sistema usando um cartão de memória ou cartão inteligente juntamente com uma senha ou PIN. Para verificação biométrica, o utilizador digita um PIN e também usa um sensor biométrico. O sistema extrai o recurso correspondente e compara isso com o modelo armazenado para esse utilizador. Se houver uma correspondência, então o sistema autentica deste utilizador;

Identificação: Neste método, o utilizador utiliza o sensor biométrico sem qualquer outra informação adicional apresentada. O sistema compara, em seguida, o modelo apresentado com o conjunto de modelos armazenados. Se houver uma correspondência, então este utilizador é identificado. Caso contrário, o utilizador é rejeitado.

Problemas de autenticação

Existem diferentes problemas de autenticação de utilizador;

- Adivinhar ou roubar senhas, PIN, etc.
- Esquecer senhas, PIN.
- Roubo ou clonagem de smartcards.

Autorização

Embora a autenticação refere-se a verificar as identidades, autorização concentra-se em determinar o que um utilizador tem permissão para fazer. É definido como privilégios de acesso concedido a um utilizador, programa ou processo "por exemplo:. Uma aplicação bancária on-line irá autenticar um utilizador com base em suas credenciais, mas deve, então, determinar as contas às quais o utilizador tem acesso. Além disso, o sistema determina as ações que o utilizador pode tomar em relação a essas contas, tais como visualização de saldos e fazer transferências.

O não-repúdio

Isto é definido como "garantia o remetente de dados é fornecido com o comprovante de entrega e o destinatário é fornecido com o comprovante de identidade do remetente, então, nem mais tarde pode negar ter processado os dados.

Conclusão

Nesta lição discutimos os diferentes metodos de autenticação e autorização de utilizadores num sistema computacional, bem como fizemos uma análise das fragilidades de cada um dos mecanismos de autenticação.

Avaliação

1. Liste os tipos de autenticação por si estudados.
2. Liste 5 características usadas em aplicações biométricas.

Actividade 1.2 - Controlo de acesso

Introdução

Nesta lição iremos discutir, os princípios de controle de acesso, bem como as políticas de controle de acesso

Detalhes da atividade

Princípios de controle de acesso

O controle de acesso coloca em prática uma política de segurança que define quem ou o quê (por exemplo, no caso de um processo) podem ter acesso a cada recurso específico do sistema e do tipo de acesso que é permitido em cada instância.

Além disso, o controle de acesso tem outras entidades e funções:

Autenticação: Este verifica se as credenciais de um utilizador ou outra entidade do sistema são válidos.

Autorização: Isso permite que uma entidade do sistema para aceder um recurso do sistema. Esta função determina quem é confiável para uma determinada finalidade.

Auditoria: Esta é uma revisão independente e análise dos registos e actividades do sistema, a fim de fazer o seguinte:

Teste para adequação dos controles do sistema;

Garantir a conformidade com a política estabelecida e procedimentos operacionais;

Detectar falhas na segurança;

Recomendar quaisquer alterações indicadas no controle, políticas e procedimentos.

Funcionamento do Mecanismo de Controle de Acesso

Um mecanismo de controle de acesso opera entre um utilizador (ou um processo de execução em nome de um utilizador) e recursos do sistema, ou seja, aplicativos, sistemas operativos, firewalls, roteadores, arquivos e bases de dados. O sistema tem que primeiro permitir a entidade que está à procura de acesso. O processo de autenticação deve primeiro determinar se o utilizador é permitido o acesso aos recursos do sistema. O controle de acesso, em seguida, determina se o acesso solicitado por que determinado utilizador é permitido. A função de controle de acesso consulta esta base de dados para determinar se concede o acesso. Uma função de monitorização mantém um registro das actividades do utilizador.

Políticas de Controle de Acesso

A política de controle de acesso determina o tipo de acesso que é permitido e em que circunstâncias e por quem esse acesso é permitido. Esta política é, por vezes, consubstanciada na base de dados de autorização. políticas de controle de acesso podem ser divididos em diferentes categorias;

Controle de acesso discricionário (DAC):

Esta categoria de política de controle de acesso é baseada em duas partes principais; A identidade do requerente e as regras de acesso (autorização), que incluem o que o requerente é permitido ou não permitido fazer. Esta política foi nomeado discricionário simplesmente porque uma entidade pode ter direitos de acesso que permitem a entidade, por sua própria vontade, para permitir uma outra entidade para acessar algum recurso.

Controle de acesso obrigatório (MAC):

Esta política é baseada na comparação entre dois itens principais; etiquetas de segurança (esses rótulos mostrar como sensível ou crítica os recursos do sistema são) e certificado de segurança (este item mostra que entidades do sistema que são qualificados para acessar determinados recursos). Esta política é designada obrigatória simplesmente porque uma entidade que tem autorização para aceder um recurso não pode, apenas por sua própria vontade, permitir que outra entidade tenha acesso a esse recurso.

Controle de acesso baseado em função (RBAC):

Esta política também se baseia em duas coisas; o papel que um utilizador tem dentro do sistema e as regras que estipulam que acessos são permitidos para utilizadors em funções dadas.

Requisitos de controle de acesso

Existem diferentes conceitos e recursos que são necessários para o sistema de controle de acesso.

Entrada de confiança: o sistema de controle de acesso requer entradas que são de fontes confiáveis. Por exemplo, este sistema assume que um utilizador é autêntico assim um sistema de autenticação é actua como um front-end para um sistema de controle de acesso. Outras entradas para o sistema de controle de acesso também devem ser confiáveis. Por exemplo, algumas restrições de controle de acesso pode depender de um endereço, como um endereço IP de origem ou o endereço de controle de acesso ao meio. O sistema geral deve ter um meio para determinar a validade da fonte para estas restrições de modo a operar eficazmente.

Suporte para as especificações finas e grossas: O sistema de controle de acesso também requer especificações de granulação fina. Esta especificação permite o acesso a ser regulada a nível de registros individuais em arquivos e campos individuais dentro de registros. Os administradores de sistema também deve ser capazes de escolher a especificação de granulação grossa para algumas classes de acesso a recursos, para reduzir a carga administrativa e de processamento do sistema

Menor privilégio: Este requisito envolve a implementação de controle de acesso de modo que cada entidade do sistema é concedido os recursos do sistema mínimos e autorizações que a entidade necessita para fazer o seu trabalho.

Separação de dever: Este requisito envolve dividir funções em uma função do sistema entre os diferentes indivíduos. Isto impede que um indivíduo de subverter o processo.

Políticas abertas e fechadas: Em uma política fechada, só acesse que são especificamente autorizados são permitidos. Em uma política aberta, as autorizações especificar quais acessos são proibidos; todos os outros acessos são permitidos.

Combinações de políticas e resolução de conflitos: É possível que o mecanismo de controle de acesso para aplicar várias políticas para uma determinada classe de recursos. Nestas circunstâncias, deve-se tomar muito cuidado para que não haja conflitos de modo que uma política permite um acesso particular, enquanto outra política nega. Ou, se existe um conflito, um procedimento deve ser definida para a resolução de conflitos.

As políticas administrativas: políticas administrativas são necessárias para determinar quem pode adicionar, excluir ou modificar as regras de autorização.

Conclusão

Esta actividade discutidos os princípios de controle de acesso diferentes, necessidades, bem como as políticas de controle de acesso.

Avaliação

1. Fale das categorias das políticas de controlo de acesso.

Actividade 1.3 - Sistemas de Detecção de Intrusão

Introdução

Existem várias tecnologias que protegem o perímetro das redes de computadores contra invasores e ameaças externas. Porém, esses sistemas não podem parar invasores que obtém acesso autenticado e usufruem do sistema como se fossem legítimos utilizadores.

Nesta lição iremos discutir os sistemas de detecção de intrusão (IDS), as formas de detecção e os tipos de IDS. Os IDS podem detectar tentativas de intrusão num sistema computacional, mas no entanto é importante resalvar que não existe uma protecção total, pois a segurança não é um estado mas sim um processo.

IDS assume que o comportamento de um atacante é diferente daquela de um utilizador legítimo. Mas, na realidade, esses comportamentos podem ser indistinguíveis. Um utilizador legítimo pode ter comportamento suspeito ou um invasor pode disfarçar seu comportamento e se passar por um utilizador legítimo.

Os objetivos de um IDS são:

- A detecção e activação dos mecanismos de resposta;
- Recuperação;
- Prevenção contra ataques futuros.

Detalhes da atividade

Princípio de funcionamento de um IDS

Duas abordagens podem ser adotadas na implementação de um IDS. Ele irá detectar qualquer comportamento anormal ou função com base em assinaturas. Um IDS que detecta um comportamento anormal vai monitorar eventos e compara-os com o comportamento em questão. Isto é feito, a fim de detectar qualquer desvio do comportamento normal. Este comportamento normal pode ser definido de uma forma global ou ao nivel do utilizador.

Numa abordagem de detecção por assinatura, os modos de acção dos ataques conhecidos estão listados e a detecção é realizada por comparação com as assinaturas. A detecção por assinatura tenta caracterizar o comportamento perigoso e detectar qualquer destes comportamentos quando ele ocorre.

A detecção por anomalias pode detectar métodos de intrusão desconhecidos. detecção de intrusões não é, no entanto, necessariamente melhor que a detecção por assinatura. A detecção de anomalias conduz comportamento normal por calibração, que pode ser ineficaz se o sistema for calibrado enquanto o intruso já efectivou a sua acção.

Tipos de Sistemas de Detecção de Intrusão

Sistemas de Detecção de Intrusão baseados em Host monitora e analisa informações coletadas de um único Host (Máquina). Não observa o tráfego que passa pela rede, seu uso volta-se a verificação de informações relativas aos eventos e registros de logs e sistema de arquivos (permissão, alteração, etc.). São instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor e os utilizadores não precisam ser monitorados. Também é aplicada em redes onde a velocidade de transmissão é muito alta como em redes "Gigabit Ethernet" ou quando não se confia na segurança corporativa da rede em que o servidor está instalado.

Sistemas de Detecção de Intrusão baseados em Rede (NIDS).

Sistemas de Detecção de Intrusão baseados em Rede monitora e analisa todo o tráfego no segmento da rede. Consiste em um conjunto de sensores que trabalha detectando atividades maliciosas na rede, como ataques baseados em serviço, portscans, etc… São instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes ou do tráfego e seus detalhes como informações de cabeçalhos e protocolos. Os NIDS tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum utilizador legítimo está fazendo mau uso do mesmo.

Sistemas de Detecção de Intrusão Híbridos

Sistemas de Detecção de Intrusão Híbridos é utilização dos sistemas baseados em redes e dos sistemas baseados em Host para controlar e monitorar a segurança computacional de um ambiente.

IDS baseados em assinaturas:

Este tipos de IDS monitoram pacotes na rede. Ele compara os pacotes que trafegam na rede com os armazenados numa base de dados de ameaças conhecidas, agindo de uma forma similar a um software antivírus. Quando uma nova ameaça aparece, esta é adicionada à base de dados com antecedência. Toda nova ameaça não é detectada até que a base de dados seja actualizada para incluir esta ameaça.

IDS baseado em anomalia:

Este tipos de IDS monitora o tráfego de rede. Ele compara o tráfego de rede com uma linha de base. Linha de base é o tráfego "normal" para a rede.

Qual é a actividade?

Conclusão

Nesta lição foram discutidos o principio de funcionamento de um IDS e sua classificação.

Avaliação

1. Liste os sistemas de detecção de intrusão por si estudados.
2. Como funciona um sistema de detecção de intrusão?

Actividade 1.4 - Firewall

Introdução

A possibilidade de conexão com a Internet traz consigo alguns riscos ás organizações (Moraes, 2010):

Relacionados aos dados (confidencialidade, integridade e disponibilidade);

Relacionados aos recursos e aos activos da organização;

Relacionados à imagem da organização, uma vez que um ataque bem sucedido pode representar um verdadeiro risco á reputação da organização caso seja divulgado.

Estes riscos ocorrem porque normalmente não existe uma política de segurança clara quanto às conexões com a Internet, e as reddes que constituem a Internet também não são seguras e confiáveis (Moraes, 2010). O firewall é um equipamento de rede que desempenha um papel fundamental dentro deste cenário.

É importante frisar que o ferewall não nos protege de ataque internos.

Detalhes da atividade

Segundo (Moraes, 2010), o firewall é um sistema que actua como ponto único de defesa entre a rede privada e a Internet. Ele pode ainda controlar o tráfego entre as sub-redes de uma rede privada.

Princípios de filtragem

Na operação de funcionamento de um firewall existem dois princípios de filtragem:

Filtragem positiva que passa apenas o tráfego que cumpre certos critérios. Qualquer tráfego indefinido será descartado.

Filtragem negativa descarta todo tráfego que cumpre determinados critérios. Qualquer tráfego indefinido será aceite.

Dependendo do tipo dos fluxos analisadas podem ser distinguidos filtragem de pacotes ou aplicação.

A filtragem de pacotes

Um firewall pode controlar o tráfego através da análise de pacotes que entram ou saem. Neste caso, as bases de dados de filtragem pode ser:

endereço IP de origem ou de destino;

Os números de porta;

A interface de rede (por exemplo, rejeitar pacotes com endereço IP interno se vier de uma interface errada).

Essa filtragem tem algumas desvantagens. Na verdade, é difícil de configurar um firewall. Por exemplo, alguns e protocolos como FTP incorporam mudanças dinâmicas durante a transferência. Erros de configuração podem ser exploradas.

Filtrando no nível do aplicativo

O firewall aparece como um proxy para os utilizadores. Qualquer conexão envolve duas conexões TCP. Uma máquina interna para o proxy e proxy para fora. Na medida em que tal filtragem pode passar por uma autenticação do utilizador, torna-se mais eficaz contra os ataques dos protocolos TCP / IP.

Um firewall não é um dispositivo que garante a segurança absoluta. Sua proteção é eficaz se ele estiver configurado e se toda a comunicação com o exterior passa através dele (estações de trabalho móveis para a Internet são potenciais furos de segurança). Na verdade, deve-se monitorar cuidadosamente o histórico de conexões para detectar tentativas de intrusão e alterar as configurações de firewall como novos modos de ataque relatados nos boletins de segurança emitidos.

DMZ

DMZ é usado para que um conjunto de serviços sejam acessíveis de fora da rede: servidor de correio, servidor de FTP, servidor web, etc. O particionamento resultante desta escolha implica

uma mudança na arquitetura de rede. Ele deve definir para cada área da rede, o qual o fluxo permitido e fluxo permitido com o mundo exterior.

Conclusão

Nesta lição falamos de firewall, assim como o principio de funcionamento dos mesmos.

Avaliação

1. O que é um firewall?
2. Como funciona um firewall?

Actividade 1.5 - Laboratório da Unidade 4

1.5.1 Laboratório

Objectivo do laboratório

Firewall

Instalar e configurar um firewall

Recursos

Debian 8.0;

VirtualBox 5.x.x

Editor vim.

Tempo

6 Horas.

Descrição do exercício

1. Instalar o VirtualBox.
2. Instalar o sistema operativo Debian.
2. Instalar o Iptables.
3. Com recurso ao editor vim configure o Iptables.
4. Inicializar e testar o Iptables.

Resultados e submissão

Submissão:

A solução deve ser submetida no final da aula laboratorial. O estudante deverá executar todas as tarefas e testá-las. Caso não termine a actividade o estudante poderá enviar o trabalho via Google Drive.

Solução

1. Aplique o patch do iptables, digite:

cd /usr/src/iptables-1.3.7

patch -p1 < ../netfilter-layer7-v2.9/iptables-layer7-2.9.patch

chmod +x extensions/.layer7-test

make KERNEL_DIR=/usr/src/linux

make install KERNEL_DIR=/usr/src/linux

Acabamos a configuração do iptables, agora temos que descompactar as definições de protocolos do layer 7, vá até a pasta onde você salvou as definições e execute:

tar xvzf l7-protocols-2007-01-14.tar.gz

Entre na pasta que você descompactou,

cd l7-protocols-2007-01-14

e execute:

make install

Está pronta a instalação do iptables e dos protocolos para layer 7.

2. Ficheiro de configuração do Iptables

iptables -t mangle -N DIVERT

iptables -t mangle -A DIVERT -j MARK --set-mark 1

iptables -t mangle -A DIVERT -j ACCEPT

iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT

iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY --tproxy-mark 0x1/0x1 --on-ip 127.0.0.1 --on-port 3128

Referências ou Links chaves

- https://www.youtube.com/watch?v=on_ka3WLXGU (Video Aula com intruções de intalação do debian)
- https://www.debian.org/CD/http-ftp/
- https://www.virtualbox.org/wiki/Downloads

Resumo da Unidade

Nesta unidade falamos dos serviços de segurança informática, onde discutimos conceitos como mecanismos de autenticação, controlo de acesso, sistemas de detecção de intrusão e firewalls.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Sede da Universidade Virtual africana

The African Virtual University
Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

Escritório Regional da Universidade Virtual Africana em Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org