Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 1: Tema - 1. PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

3 Objetivos

- Conhecer a história e evolução da segurança cibernética, possibilitando estabelecer comparações entre os cenários passados e atuais

- Entender o valor da informação para o negócio e pessoas, compreendendo os motivos pelos quais o melhor esforço para sua proteção deve ser preservado.

4 Tópicos

1.1 EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA
1.2 VALOR DA INFORMAÇÃO - ALINHAMENTO ESTRATÉGICO DA SEGURANÇA AOS NEGÓCIOS

5 Procedimentos de ensino-aprendizagem

- Situação problema
Parques tecnológicos são constituídos para auxiliar e agilizar a gestão e processamento de todas informações úteis para a empresa. Estas informações geram valor para a empresa, viabilizando negócios, planejamentos comerciais, estratégias de marketing, projetos de produtos, dentre outros. Tempos atrás, antes da interligação entre dispositos e empresas através da internet, estas informações não eram facilmente acessíveis devido ao isolamento existente, o que não ocorre atualmente, já que uma empresa pode ter seu ambiente de rede acessado sem autorização, o que proporcionou o surgimento da preocupação com a salvaguarda destes dados, originando o surgimento da área de segurança cibernética. Voce sabe mensurar o valor informação para uma empresa e os impactos que o comprometimento desta representa para o negócio?

- Metodologia
Conforme [1], sugere-se ao docente apresentar aos alunos os princípios basilares da informação, produzindo vinculo entre estes e o que representam para o negócio da empresa, bem como o impacto representativo de sua não observância, bem como os modelos de segurança e desafios inerentes à área. Utilizando [2] expor aos alunos a evolução da história da segurança da informação e a forma como estas eram comprometidas no passado

- Verificação de Aprendizado
Com auxilio do docente, oferecer aos alunos, em trabalho conjunto, a criação de 1 ou 2 cenários negativos, do ponto de vista de segurança, quais princípios seriam afetados e qual o impacto no funcionamento do negócio.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Stallings, William, William Stallings, Lawrie Brown - Segurança de computadores : princípios e práticas [tradução Arlete Simille Marques]. - 2. ed. - Rio de Janeiro : Elsevier, 2014. Páginas 7 a 9

[2] Basta, Alfred Segurança de computadores e teste de invasão / Alfred Basta, Nadine Basta e Mary Brown ; tradução Lizandra Magon de Almeida. - São Paulo : Cengage Learning, 2014. Páginas 1 a 11

8 Aprenda +

1) O que é Segurança da Informação? - Disponível em: https://youtu.be/_OrtR-qR_mw
2) Segurança informação video 01 - Disponível em: https://youtu.be/ZD66EMgB1FA
3) Segurança Cibernética: Funcionamento e Exemplos - Disponível em: https://youtu.be/mLWd6kO2Udk
4) Você sabe o que é CIBERSEGURANÇA? - Disponível em:https://youtu.be/CU2yQxzkvFg

Atividade Autônoma Aura:

Questão 1:
Desde antes da popularização da internet já era de conhecimento comum que os sistemas operacionais tinham vulnerabilidades. Falando do começo da década de 90, as guerras cibernéticas eram travadas entre os antivírus e os conteúdos que vinham em disquetes, principais vetores de aplicações maliciosas. A internet surgiu e ganhou o mundo e os dias das pessoas, facilitando o dia a dia da humanidade, inclusive das pessoas mal-intencionadas, que utilizam a rede mundial para atacar sistemas. Do lado da defesa contra atividades ilegais, estão profissionais especializados em analisar vulnerabilidades e indicar soluções.

Com base no texto, a ação de ataque contratado por uma empresa para atacar seu parque tecnológico e tentar encontrar falhas é conhecida como:

Alternativas:
A) Pentesting
B) XSS
C) Arp spoofing
D) Metaexploit

E) SQL

Questão 2:
São gastos bilhões em tecnologia. Esta frase é comum de se ler em revistas especializadas em Gestão em tecnologia da informação. As empresas têm sua história construída, baseada e mantida sobre contatos com clientes, fornecedores, históricos de movimentações financeiras e de estoque, bem como ações e estratégias de marketing e desenvolvimento de novos produtos ou serviços. Se tudo se perder, é melhor a empresa fechar as portas!

Com base no texto, é considerado o ativo mais importante de uma empresa.

Alternativas:

A) Os storages
B) Os servidores
C) O datacenter
D) A informação
E) Os funcionários

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 2: Tema - 1. PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

3 Objetivos

- Conhecer os principais mecanismos de proteção da informação, de forma que seja possível indicar as melhores soluções para cada cenário

4 Tópicos

1.3 INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS

5 Procedimentos de ensino-aprendizagem

- Situação problema
A área de tecnologia deduz a necessidade de investimentos, muitas vezes, grandiosos para obtenção, processamento e gestão das informações, o que inclui investimentos para protegê-las. Quando a palavra proteção entra em cena, muitos pensam em hackers e ataques, quando, na verdade, a palavra "proteção" submete à tarefas como manter a informação sempre disponível e confiável, o que não tem relação direta ou frequente com acesso indevido, roubo ou sequestro de dados, mas, sim, com backups, redundância, treinamento de pessoal e outras atividades. Voce teria noção do que precisa ser feito e os equipamentos necessários para garantir o sucesso de tantas atividades? Saberia mensurar, em valores, o montante necessário para proteção adequada dos dados?

- Metodologia
Com base em [1], sugere-se que o docente apresente aos alunos quais as informações que necessitam de atenção e o nível de cuidado demandado por cada uma. Utilizando [2] abordar a atividade de preparação do corpo de recursos humanos contra atividades de engenharia social. Com base em [3], apresentar superficialmente alguns tipos de ataques e o que precisa ser feito para diminuir a chance de sucesso destes

- Verificação de Aprendizado
Com a mediação do Docente e posterior validação, formar grupos para enumeração de equipamentos de tecnologia que componham um parque tecnológico de porte intermediário, quais os tipos de informações que ali existem, seus possíveis vulnerabilidades quais seriam os equipamentos necessários para sua proteção, utilizando pesquisa na internet para obtenção de valores destes para formação do

montante necessário de investimento

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Basta, Alfred Seguranc¸a de computadores e teste de invasa~o / Alfred Basta, Nadine Basta e Mary Brown ; traduc¸a~o Lizandra Magon de Almeida. - São Paulo : Cengage Learning, 2014. - Pagina 11

[2] Basta, Alfred Seguranc¸a de computadores e teste de invasa~o / Alfred Basta, Nadine Basta e Mary Brown ; traduc¸a~o Lizandra Magon de Almeida. - São Paulo : Cengage Learning, 2014. - Pagina 26

[3] Basta, Alfred Seguranc¸a de computadores e teste de invasa~o / Alfred Basta, Nadine Basta e Mary Brown ; traduc¸a~o Lizandra Magon de Almeida. - São Paulo : Cengage Learning, 2014. - Pagina 84 e 99

8 Aprenda +

1) 5 ferramentas de segurança para proteger sua rede! - Dispoinível em: https://youtu.be/CInn1mpc67M

2) Como dimensionar os equipamentos de segurança em sua rede - Dispoinível em: https://youtu.be/fw1tVXBURDk

Atividade Autônoma Aura:

Questão 1:
Um parque tecnológico tem servidores para controlar a rede, bem como fornecer os serviços necessários ao ambiente para processamento das informações. Estes dados precisam ficar no datacenter, local que abarca todos os equipamentos importantes de uma rede.

Com base no texto, dentre todos os equipamentos de um datacenter há aquele responsável por armazenar todas as informações de uma rede. Este equipamento é:

Alternativas:
A) Os storages
B) Os servidores
C) O datacenter
D) O Switch

E) A topologia estrela

Questão 2:
Um parque tecnológico tem servidores para controlar a rede, bem como fornecer os serviços necessários ao ambiente para processamento das informações. Para facilitar a organização, é prudente que todos os equipamentos mais importantes fiquem em um único local, seguro e apropriado para recebê-los.

Com base no texto, temos que o local de concentração dos dispositivos importantes de uma rede de computadores é conhecido como:

Alternativas:

A) Os storages
B) Os servidores
C) O datacenter
D) O Switch
E) A topologia estrela

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 3: Tema - 1. PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

3 Objetivos

- Identificar os serviços que serão disponibilizados na rede, para definir as ameaças às quais estarão submetidos, tornando possível elencar as ferramentas de segurança que devem ser utilizadas.

4 Tópicos

1.4 PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

5 Procedimentos de ensino-aprendizagem

- Situação problema
Conhecer o que está sendo trabalhado é uma obrigação. Na área de tecnologia trata-se de garantir a sobrevivência. Conhecer o parque tecnológico de um negócio é indispensável, pois possibilita tomar ciência das soluções para que uma análise de possíveis vulnerabilidades seja providenciada. Com base nesta análise, torna-se viável a construção de um plano de segurança mas, paar isto, é necessário conhecer detalhes técnicos consistentes sobre o funcionamento de sistemas operacionais, aplicações e redes de computadores. Voce sabe pesquisar vulnerabilidades de soluções? Sabendo das vulnerabilidades de um ambiente, teria condições de encontrar possíveis formas de contorna-las ou resolve-las?

- Metodologia
Com base em [1] apresentar aos alunos como ocorre o fluxo de informações entre dispositivos, possibilitando aos alunos entenderem como as conexões são estabelecidas emtre dispositivos. Utilizando [2] apresentar os requisitos de segurança para ambientes tecnológicos, uma vez que são estes requisitos que irão direcionar os profissionais durante a produção de um plano de segurança.

- Verificação de Aprendizado
Com a mediação do Docente e posterior validação, convidar os alunos a construir uma lista com os serviços de rede mais usados e, utilizando a ferramenta [3], definir quais as principais vulnerabilidades

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Forouzan, Behrouz A. Redes de computadores [recurso eletrônico] : uma abordagem top-down / Behrouz A. Forouzan, Firouz Mosharraf ; tradução técnica: Marcos A. Simplicio Jr., Charles Christian Miers. Dados eletrônicos. Porto Alegre : AMGH, 2013. - Paginas 34 a 42

[2] Stallings, William, William Stallings, Lawrie Brown - Segurança de computadores : princípios e práticas [tradução Arlete Simille Marques]. - 2. ed. - Rio de Janeiro : Elsevier, 2014.- Página 19

[3] - Miro - Disponível em: https://miro.com/education-whiteboard/

8 Aprenda +

1) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM 5 PASSOS - Dispoinível em: https://youtu.be/nI1o-w4nKdc

2) Cybersecurity Projects - Find a Project and Create the Plan - Dispoinível em: https://youtu.be/kGt9hHoybFg

Atividade Autônoma Aura:

Questão 1:
As empresas começam assim: ocorre uma reunião da diretoria executiva com os consultores de T.I. Nesta reunião são elencadas as necessidades da empresa, para que os consultores possam analisar e informar quais soluções atendem às necessidades informadas, bem como o que será necessário fazer para mantê-las ao longo do tempo de vida da empresa. Afinal, é de conhecimento de todos que a informação é o ativo mais valioso de uma empresa.

Com base no texto, o plano cuja finalidade é salvaguardar as informações de uma empresa contra ataques diversos, inundações, incêndios, etc é conhecido como:

Alternativas:
A) Storage plan
B) Security plan
C) Datacenter plan
D) Network plan
E) Information Plan

Questão 2:
Um ambiente computacional profissional, como o das grandes empresas, necessita de muito mais do que apenas vários computadores, pois precisam de um ambiente complexo e potente para armazenar,

processar e disponibilizar saídas consolidadas do dia a dia da empresa, porque é a análise do resultado do processamento destas informações que irá orientar as tomadas de decisões e estratégias mercadológicas no futuro. Por conter informações tão valiosas, muitas vezes valendo milhões. O alto valor dos dados coloca em risco as informações, pois desafetos, concorrentes ou simples pessoas mal-intencionadas podem estar de olho neste ativo, para fins comerciais, sequestro de dados, bem como qualquer outro motivo. Todos injustificáveis e errados! Isto faz com que a empresa precise se preocupar com a salvaguarda de seus ativos.

Com base no texto, o plano cuja finalidade é salvaguardar as informações de uma empresa contra ataques diversos, inundações, incêndios, etc é conhecido como:

Alternativas:
A) Storage plan
B) Network plan
C) Datacenter plan
D) Security plan
E) Information Plan

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 4: Tema - 2. AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES

3 Objetivos

- Conhecer as principais ferramentas de interceptação de pacotes e de reconhimento de rede, possibilitando o combate a possíveis problemas de exposição de tráfego.

4 Tópicos

2.1 INTERCEPTAÇÃO DE TRÁFEGO & MAPEAMENTO DE REDES

5 Procedimentos de ensino-aprendizagem

- Situação problema
O fluxo de informação entre dispositivos circula em meio onde existem outros equipamentos também conectados. Com a utilização de técnicas de interceptação, é possível capturar os dados, utilizando programa de captura de pacotes instalado em um dos equipamentos envolvidos na comunicação, ou instalado em terceiro dispositivo não envolvido na transmissão. Para o primeiro caso isto é utilizado para o entendimento e solução de possíveis problemas na transmissão e no outro, muitas vezes, para interceptação não autorizada do fluxo. Os programas que fazem este tipo de captura são conhecidos como sniffers (farejadores) de rede. Contudo, a utilização correta destes programas exige conhecimento consistente e profundo do profissional. Voce conhece algum destes programas? Saberia como operá-los?

- Metodologia
Com base em [1], sugere-se que o Docente informe aos alunos sobre os tipos de sniffers de rede e suas funcionalidades, utilizando [2] para informe de serviços de rede e respectivas portas de serviço.

- Verificação de Aprendizado
Sugere-se a utilização de um programa sniffer de rede, especificamente o wireshark, para proceder com a captura de pacotes com base no endereço IP, posteriormente capturando fluxo de dados em apenas uma porta específica, bem como dados vindos de uma rede IP específica, independente do endereço IP, dentre outras implementações e variações de captura, sempre procedendo com a análise do que fora capturado.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] BASTA Alfred. Segurança de Computadores e Testes de Invasão. 2ª edição. São Paulo: Editora Trilha, 2015. - Páginas 43 a 45 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366

[2] Forouzan, Behrouz A. Redes de computadores [recurso eletrônico] : uma abordagem top-down / Behrouz A. Forouzan, Firouz Mosharraf ; tradução técnica: Marcos A. Simplicio Jr., Charles Christian Miers. " Dados eletrônicos." Porto Alegre : AMGH, 2013. - Páginas 43 a 82 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788580551693/cfi/1!/4/4@0.00:66.9

8 Aprenda +

1) How to Intercept IP Connections in a Malware Analysis Lab - Dispoinível em: https://youtu.be/1KBv1Yp78qM

2) Sniffing - Segurança da Informação - Dicionário de Informática - Dispoinível em: https://youtu.be/yZdhAXMWw-c

3) [aXR6] - badKarma - Kit de Ferramentas Avançadas de Reconhecimento de Rede - Dispoinível em: https://youtu.be/oQMCwh4NMsI

Atividade Autônoma Aura:

Questão 1:
As informações fluem entre os dispositivos através de cabos, fibra e do ar. Independente do meio, são passíveis de interceptação por terceiros não autorizados através de aplicação de várias técnicas direcionando o fluxo para o dispositivo invasor, que as recebe e consegue acesso ao que estava sendo transmitido, muitas vezes sem que as partes envolvidas desconfiem do que está acontecendo.

Com base no texto, é um programa que pode ser utilizado para capturar pacotes e remontá-los:

Alternativas:
A) MySql
B) SQL
C) Linux
D) Event viewer
E) Wireshark

Questão 2:
Com o surgimento da internet e as facilidades que trouxe à humanidade, vieram os problemas relacionados à segurança, já que muitas soluções se tornaram alcançáveis a pessoas mal-intencionadas, através da rede mundial. Uma das etapas de invasão de ambientes trata reconhecer a rede e os ativos nela disponíveis para, posteriormente, tentar obter acesso às informações neles contida.

Com base no texto, é ferramenta que ode ser utilizada para o mapeamento de uma rede e reconhecimento dos sistemas e serviços nela disponíveis

Alternativas:
A) nmap
B) ping
C) traceroute
D) Wireshark
E) Active directory

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 5: Tema - 2. AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES

3 Objetivos

- Conhecer o funcionamento de aplicações web e algumas de suas vulnerabilidades, para prever possíveis pontos de vulnerabilidade

- Entender a produção e as diversas finalidades de códigos maliciosos, para compreender como operam durante a exploração de sistemas e aplicações

- Entender o processo de engenharia social e seus alvos potenciais, possibilitando a prevenção de exposição de informações desnecessárias

4 Tópicos

2.2 ATAQUES E VULNERABILIDADES DE APLICAÇÕES WEB
2.3 CÓDIGOS MALICIOSOS

5 Procedimentos de ensino-aprendizagem

- Situação problema
A rede mundial de computadores veio para integrar a humanidade, os equipamentos e prover agilidade no fluxo de informações. Contudo, junto das facilidades veio o perigo da exposição de dados sensíveis. Em um mundo onde a informação tem alto valor, qualquer meio através do qual ela possa ser obtida torna-se uma ótima oportunidade. Em geral, as pessoas interagem com sites, depositando partes importantes de seus dados pessois, que são armazenados em bancos de dados para uso posterior das mais diversas formas. Sites e bancos de dados, por manterem algum tipo de acesso via internet, tornam-se alvos substanciais de pessoas mal-intencionadas. Por outro lado, existem técnicas que exploram a boa-fé e o descuido das pessoas para obtenção de informações. Voce saberia enumerar quais seriam os perigos aos quais estes serviços estão expostos?

- Metodologia
Utilizando [1], sugere-se que o Docente apresente aos alunos quais são algumas das vulnerabilidades às quais os serviços WEB estão expostos. Com base em [2] falar sobre engenharia social, expondo aos alunos a importância da Conscientização, treinamento e educação de segurança.

- Verificação de Aprendizado

Junto aos alunos, com uso de [3] construir uma lista com os serviços WEB mais utilizados, suas integrações e possíveis pontos de falhas. Por fim, sugere-se que seja feito uma pequena encenação de situações onde é possível utilizar engenharia social.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] SCAMBRAY, Joel; McCLURE, Stuart; KURTZ, George. Hackers Expostos: Segredos e Soluções para a Segurança de Redes. 4ª edição. Porto Alegre: Editora Bookman, 2014. - Páginas 555 a 568 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601426

[2] STALLINGS, William. Segurança de Computadores - Princípios e Práticas. 2ª edição. Rio de Janeiro: Editora Elsevier, 2014. - Página 501 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459

[3] - Miro - Disponível em: https://miro.com/education-whiteboard/

8 Aprenda +

1) Vulnerabilidades em aplicações web - Disponível em: https://youtu.be/oaxYwTk3AoE
2) Reconhecimento Web e Vulnerabilidades - Introdução ao Hacking e Pentest - Solyd - Disponível em: https://youtu.be/wdysXk6Jsbk
3) Ferramenta automatizada para identificação de vulnerabilidades web - Disponível em: https://youtu.be/EIaNa_Rwck8

Atividade Autônoma Aura:

Questão 1:
Antigamente, quando uma solução precisava ser disponibilizada para usuários, era necessário instalar um programa nos computadores, o que não ocorre mais hoje em dia, já que as soluções são disponibilizadas através de páginas de internet, utilizando as mais diversas tecnologias, como PHP, JSP, Python, GoLang, entre outras. Assim, basta que o usuário acesse a URL da solução para que possa fazer uso. Contudo, o fato de a solução estar disponível através da internet e utilizando diversas tecnologias a coloca em risco, pois é necessário que os desenvolvedores da solução atentem para possíveis vulnerabilidades nas tecnologias que estão sendo empregadas, sendo necessário recorrer à ambientes de colaboração online específicos.

Com base no texto, ao escolher um ambiente ou tecnologia para disponibilizar ou desenvolver uma solução, é preciso buscar por alguma vulnerabilidade já conhecida, a qual é identificada como:

Alternativas:
A) CSV
B) CVE
C) HTTP
D) WWW
E) HTML

Questão 2:
Apesar das cifras milionárias investidas em segurança da informação, ativo de maior valor de uma empresa, onde equipamentos de última geração são comprados, como: firewalls, antispam, antivírus e excelentes profissionais de T.I., os problemas relacionados à segurança continuam, devido à exploração de um ponto fraco presente em todos os lugares, que são as pessoas, as quais acessam URLS indevidas, executam arquivos proibidos, conectam pendrives infectados, divulgam informações ou pistas de dados sensíveis em redes sociais, dentre outros comportamentos que deveriam ser evitados. O resultado disto é que todo investimento se torna sem efeito, pois o ambiente será colocado em risco, independente da cifra investida em segurança.

Com base no texto, é técnica que explora as diversas fraquezas de funcionários de empresas:

Alternativas:

A) OWASP
B) BYOD
C) Engenharia social
D) Trojan
E) Worm

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 6: Tema - 2. AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES

3 Objetivos

- Conhecer as principais tecnologias wireless, suas características e modo de funcionamento, provendo entendimento sobre as formas de proteção e possíveis vulnerabilidades para esta tecnologia

4 Tópicos

2.4 WIRELESS HACKING

5 Procedimentos de ensino-aprendizagem

- Situação problema
A incessante busca do homem pelo conforto e facilidades trouxe a necessidade de liberar-se dos fios que ancoravam seus dispositivos em locais específicos, nascia a mobilidade - que é a capacidade de um dispositivo manter-se conectado à rede mesmo em movimento. Assim, livre de fios, é possível conectar-se com outros dispositivos através do ar. Para isto, basta ter um equipamento conhecido como access point, que emite um sinal de rádio com alcance limitado e todo equipamento ao alcance deste sinal poderá ingressar na rede sem fio, que pode ter senha, ou não, sendo aconselhável protege-la por senha. Voce saberia informar se uma rede wifi protegida por senha é inviolável? Conhece os mecanismos de proteção de redes sem fio?

- Metodologia
Com base em [1], sugere-se que o Docente apresente os conceitos de segurança e os pontos importantes relacionados à segurança de redes wireless. Utilizando [2] introduzir os alunos aos principais tipos de ataques a redes wifi e clientes de redes sem fio. Utilizar [3] informar aos alunos quais os principais meios e ferramentas disponíveis para implementação de segurança em redes sem fio

- Verificação de Aprendizado
A atividade descrita abaixo computará 3 pontos para a AV1.
Com a mediação do Docente e posterior validação, formar grupos para a configuração do zero de um roteador sem fio, em um cenário Cisco Packet Tracer, conforme [4] e [5], aplicando configurações não seguras. Depois os cada grupo deve redigir um documento explicando formas de meios de invasão a

esta rede, para fins de estudo e consolidação do conhecimento. Por fim, cada grupo deve proceder com as configurações adequadas de segurança adequadas estudadas durante a aula, e redigir novo documento explicando como as configuração adicionais evitam as formas de invasão citadas na primeira parte da atividade.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] WRIGHTSON, Tyler. Segurança em Redes sem Fio: Guia do Iniciante. 1ª edição. Porto Alegre: Editora Bookman, 2013. - Página 18 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601556

[2] WRIGHTSON, Tyler. Segurança em Redes sem Fio: Guia do Iniciante. 1ª edição. Porto Alegre: Editora Bookman, 2013. - Página 81 e 107 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601556

[3] STALLINGS, William. Segurança de Computadores - Princípios e Práticas. 2ª edição. Rio de Janeiro: Editora Elsevier, 2014. - Página 669 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459

[4] Vídeo "Roteador Wireless no Packet Tracer - Parte 1", Disponível em https://www.youtube.com/watch?v=6BvpG_aWE50 (Acessar usando o Chrome, e ativar a legenda e a tradução automática para Português)

[5] Vídeo "Roteador Wireless no Packet Tracer - Parte 12 , Disponível em https://www.youtube.com/watch?v=3fdy2sIbfaI (Acessar usando o Chrome, e ativar a legenda e a tradução automática para Português)

8 Aprenda +

1) Cracking WiFi WPA2 Handshake - Disponível em:https://youtu.be/WfYxrLaqlN8 (Ativar legenda automática)

Atividade Autônoma Aura:

Questão 1:
A necessidade do homem em utilizar seu equipamento de onde estiver e conseguir manter sua conectividade com a rede da empresa ou com a rede mundial de computadores foi atendida: surgiu a rede sem fio. Com esta tecnologia uma pessoa equipada com um dispositivo que tenha uma antena de tecnologia compatível, consegue se conectar ao sinal de um access point que esteja disponível na

proximidade. Contudo, é necessário proteger as redes sem fio, evitando que pessoas não autorizadas se conectem à rede, obtendo acesso aos demais dispositivos que também estão conectados à mesma rede, bem como não consigam ter acesso fácil e legível às informações que trafegam pelo ar.

Com base no texto, é mecanismo de proteção mais atual de redes wireless

Alternativas:
A) MD5
B) WEP
C) TLS
D) WPA2
E) SSL

Questão 2:
Uma empresa disponibiliza um servidor WEB em sua DMZ para que clientes e parceiro possam interagir diretamente com o conteúdo da empresa, efetuando compras, por exemplo. Um invasor, em uma ação de reconhecimento, identifica que o servidor WEB, mal configurado, retorna a versão do mecanismo, respondendo: apache 2.4.3.

Com base no texto e o caso apresentado, caso o invasor queira saber das falhas desta versão, utilizando o termo técnico adequado, deverá procurar pelo:

Alternativas:

A) LAMP do apache 2.4.3
B) CVE do apache 2.4.3
C) Módulo do apache 2.4.3
D) OWASP do apache 2.4.3
E) Honey pot do apache 2.4.3

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 7: Tema - 3. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (ATIVIDADE PRÁTICA SUPERVISIONADA)

3 Objetivos

- Identificar as principais soluções web e seu funcionamento, possibilitando a enumeração de suas possíveis vulnerabilidades

- Conhecer ataques de injeção de códigos e quebra de autenticação, para que seja possível combater as possíveis causas e diminuir a margem de risco das aplicações

4 Tópicos

3.1 INJEÇÃO, QUEBRA DE AUTENTICAÇÃO, E EXPOSIÇÃO DE DADOS SENSÍVEIS

5 Procedimentos de ensino-aprendizagem

Nesta aula, estaremos conectados com o conteúdo digital. O aluno explora e estuda, previamente, o conteúdo digital disponível em seu ambiente virtual.

6 Recursos didáticos

A aula será realizada no ambiente virtual de aprendizagem.

7 Leitura específica

O aluno deverá consultar a bibliografia proposta no tema.

8 Aprenda +

O aluno deverá aprofundar os seus estudos navegando no explore + disponível no tema digital.

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 8: Tema - 3. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (ATIVIDADE PRÁTICA SUPERVISIONADA)

3 Objetivos

- Entender a linguagem XML e seu vínculo com aplicações web, possibilitando identificar em qual ponto esta linguagem pode configurar risco à aplicações.

- Conhecer sistemas de acesso e sua forma de controle de operações, de forma a compreender como é possível ignora-los para obter acesso não autorizado à ambientes restritos

4 Tópicos

3.2 ENTIDADES EXTERNAS DE XML, QUEBRA DE CONTROLE DE ACESSOS, CONFIGURAÇÕES DE SEGURANÇA INCORRETAS

5 Procedimentos de ensino-aprendizagem

Nesta aula, estaremos conectados com o conteúdo digital. O aluno explora e estuda, previamente, o conteúdo digital disponível em seu ambiente virtual.

6 Recursos didáticos

A aula será realizada no ambiente virtual de aprendizagem.

7 Leitura específica

O aluno deverá consultar a bibliografia proposta no tema.

8 Aprenda +

O aluno deverá aprofundar os seus estudos navegando no explore + disponível no tema digital.

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 9: Tema - 3. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (ATIVIDADE PRÁTICA SUPERVISIONADA)

3 Objetivos

- Entender a comunicação entre aplicações distintas e a forma como tratam dados recebidos, provendo capacidade para o aluno entender a desserialização insegura, ou não prevista, de informações que não deveriam ser aceitas para processamento

- Conhecer como funcionam as tecnologias web estáticas e dinâmicas, bem como os aplicativos de navegação, para compreensão de como um ataque XSS pode ser bem sucedido, bem como seus riscos

4 Tópicos

3.3 CROSS-SITE SCRIPTING, DESSERIALIZAÇÃO INSEGURA

5 Procedimentos de ensino-aprendizagem

Nesta aula, estaremos conectados com o conteúdo digital. O aluno explora e estuda, previamente, o conteúdo digital disponível em seu ambiente virtual.

6 Recursos didáticos

A aula será realizada no ambiente virtual de aprendizagem.

7 Leitura específica

O aluno deverá consultar a bibliografia proposta no tema.

8 Aprenda +

O aluno deverá aprofundar os seus estudos navegando no explore + disponível no tema digital.

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 10: Tema - 3. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (ATIVIDADE PRÁTICA SUPERVISIONADA)

3 Objetivos

- Identificar as principais ferramentas de monitoramento e registro de atividades, possibilitando a devida indicação dos cenários para apropriados para sua utilização e seus benefícios

- Conhecer os riscos ao qual estão expostos ambientes sem monitoramento adequado, proporcionando entendimento sobre os impactos negativos sobre um ambiente durante um sinistro.

4 Tópicos

3.4 REGISTRO E MONITORIZAÇÃO INSUFICIENTE

5 Procedimentos de ensino-aprendizagem

Nesta aula, estaremos conectados com o conteúdo digital. O aluno explora e estuda, previamente, o conteúdo digital disponível em seu ambiente virtual.

6 Recursos didáticos

A aula será realizada no ambiente virtual de aprendizagem.

7 Leitura específica

O aluno deverá consultar a bibliografia proposta no tema.

8 Aprenda +

O aluno deverá aprofundar os seus estudos navegando no explore + disponível no tema digital.

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 11: Tema - 4. CONTRAMEDIDAS E HARDENING

3 Objetivos

- Conhecer as principais ferramentas de segurança para ambientes computacionais, possibilitando a indicação correta dos cenários onde cada uma pode ser utilizada

- Entender o funcionamento do mecanismo criptográfico e sua aplicação, para compreensão de sua aplicabilidade, benefícios e pontos fracos

4 Tópicos

4.1 FERRAMENTAS DE SEGURANÇA & CRIPTOGRAFIA

5 Procedimentos de ensino-aprendizagem

- Situação problema
O que circula entre dispositivos? Praticamente tudo! Muitas vezes não é nada importante, mas existem momentos em que o fluxo contém informações confidenciais. De qualquer maneira, os dados, sejam quais forem, não devem ser expostos, nem capturados. Para garantir isto, as empresas investem uma cifra considerável em equipamentos de segurança, atualizações de software e treinamento de pessoal e, mesmo assim, ainda é necessária a adição de uma camada complicadora, trata-se da criptografia, que é o embaralhamento do conteúdo originalmente legível de alguma informação. Existem diversos tipos de criptografia, todas elas patrocinadas por algoritmos dos mais variados. Voce sabe quais os dois tipos basilares de criptografia existentes? Sabe citar o nome de alguns algoritmos?

- Metodologia
Com base em [1] apresentar as técnicas de segurança com uso de criptografia, seguindo [2] para abordagem referente aos tipos de criptografia existentes. Utilizando [3] apresente aos alunos os principais algoritmos criptográficos.

- Verificação de Aprendizado
A atividade descrita abaixo computará 2.5 pontos para a AV2.
Como forma de fixação do aprendizado, sugere-se criar grupos de alunos que devem utilizar de um programa de captura de pacotes, inicialmente fazendo a captura de um fluxo de dados não

criptografado como, por exemplo, HTTP e, em seguida, executar outra captura, desta vez com fluxo de dados HTTPS. O docente deve apoiar a atividade, apoiando os grupos durante a análise comparativa entre as duas capturas. Ao final, cada grupo deve escrever um relatório técnico explicando a diferença entre as duas capturas, e relacionando como, por exemplo, aplicações de transações bancárias que usam HTTPS são mais seguras.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Comer, Douglas E. Redes de computadores e internet [recurso eletro^nico] / Douglas E. Comer ; traduc¸a~o: Jose´ Valdeni de Lima, Valter Roesler. 6. ed. Porto Alegre : Bookman, 2016. Página 451 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/cfi/1!/4/4@0.00:63.6

[2] Comer, Douglas E. Redes de computadores e internet [recurso eletro^nico] / Douglas E. Comer ; traduc¸a~o: Jose´ Valdeni de Lima, Valter Roesler. 6. ed. Porto Alegre : Bookman, 2016. Página 452 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/cfi/1!/4/4@0.00:63.6

[3] STALLINGS, William. Segurança de Computadores - Princípios e Práticas. 2ª edição. Rio de Janeiro: Editora Elsevier, 2014. Páginas 575 e 607 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459

8 Aprenda +

1) 5 ferramentas de segurança para proteger sua rede! - Disponível em: https://youtu.be/CInn1mpc67M

2) Criptografia (Guia Básico para Entender Como Funciona) - Disponível em:https://youtu.be/qHFbuXpz7e4

3) Criptografia | Nerdologia Tech - Disponível em:https://youtu.be/_Eeg1LxVWa8

Atividade Autônoma Aura:

Questão 1:
Através das redes de dispositivos, seja a rede mundial, ou uma rede privada, circulam informações das mais variadas, incluindo aquelas com dados que não podem ser modificados. Para garantir a integridade destas informações, há mecanismo apropriado, cujo objetivo é executar um cálculo sobre o conteúdo de um determinado arquivo e gerar um resultado. Com a utilização desta ferramenta, caso

um conteúdo seja modificado entre origem e destino, é possível verificar se ele foi modificado.

Com base no texto acima, podemos afirmar que está sendo feita referência à tecnologia

Alternativas:
A) Firewall
B) Antispam
C) criptografia
D) Hash
E) antivirus

Questão 2:

Através das redes de dispositivos, seja a rede mundial, ou uma rede privada, circulam informações das mais variadas, incluindo aquelas com dados sigilos. Para dificultar o acesso de terceiros não-autorizados à estas informações, existem mecanismos dos mais diversos. Com a utilização destes, caso um invasor tenha acesso aos dados, estes serão inelegíveis, tornando a informação desinteressante.

Com base no texto acima, são tecnologias que tornam a informação inelegível para invasores:

Alternativas:

A) Firewall
B) Antispam
C) criptografia
D) Hash
E) antivirus

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 12: Tema - 4. CONTRAMEDIDAS E HARDENING

3 Objetivos

- Identificar os campos de cabeçalho de alguns protocolos mais utilizados, bem como seu funcionnamento em ambiente computacional, para reconhecimento de possiveis falhas de segurança oriundas de configurações inadequadas

- Conhecer as sugestões de melhores práticas para configuração de alguns protocolos, diminuindo substancialmente a possibilidade de sucesso na exploração das informações destes serviços.

4 Tópicos

4.2 SEGURANÇA NOS PROTOCOLOS: IP, TCP, UDP, DNS E HTTP
4.3 HARDENING: SEGURANÇA EM AMBIENTES LINUX E WINDOWS

5 Procedimentos de ensino-aprendizagem

- Situação problema
A comunicação entre dispositivos é regida com base no tipo de dado que está sendo transferido, pois cada tipo utiliza um protocolo específico. É sabido que um protocolo contém campos de controle que são utilizados durante a formação de cada pacote que é transmitido e, neste ponto, é possível que existam falhas que podem ser oportunamente exploradas. Assim, em algumas situações é apropriado que o profissiona de T.I. proceda com ajustes adequados dos sistemas operacionais e serviços de forma a diminuir e, até, eliminar completamente os riscos aos quais um serviço pode ser submetido, técnica conhecida como hardening. Voce conhece profundamente o cabeçalho de algum protocolo? Saberia proceder com a aplicação de hardening eu algum sistema operacional ou serviço?

- Metodologia
Com base em [1] é sugerível que o Docente introduza os alunos ao estudo dos cabeçalhos dos principais protocolos de redes e o estudo superficial da finalidade de alguns de seus campos de cabeçalhos. Com base em [2] explicar e apresentar algumas falhas básicas de configuração de serviços e formas mais adequadas de configuração ou seu aprimoramento (hardening)

- Verificação de Aprendizado
Sugere-se que o Docente utilize o serviço DNS como exemplo, onde apresentará aos alunos análise de configuração deste serviço, abordando a configuração de permissão de atualização automática não

segura de sua base de dados, bem como a configuração de transferência de zona. Como sugestão adicional, o Docente poderá abordar o protocolo SNMP que, mal configurado, pode repassar informações sobre as contas locais de um sistema operacional.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Forouzan, Behrouz A. Redes de computadores: uma abordagem top-down / Behrouz A. Forouzan, Firouz Mosharraf ; tradução técnica: Marcos A. Simplicio Jr., Charles Christian Miers. "Dados eletrônicos". Porto Alegre : AMGH, 2013. Páginas 43 a 82 - Disponivel em: https://integrada.minhabiblioteca.com.br/#/books/9788580551693/cfi/1!/4/4@0.00:66.9

[2] SCAMBRAY, Joel; McCLURE, Stuart; KURTZ, George. Hackers Expostos: Segredos e Soluções para a Segurança de Redes. 4ª edição. Porto Alegre: Editora Bookman, 2014. - Páginas 225 a 229 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601426

8 Aprenda +

1) Hardening - Introdução - Disponível em:https://youtu.be/wPkYN5shNEg
2) Conceitos básicos de Hardening - Disponível em:https://youtu.be/FmB59AV4LSg

Atividade Autônoma Aura:

Questão 1:
Para fazer uso da capacidade de processamento de um computador, é necessária a instalação de um sistema operacional, seja Windows ou Linux. Sobre este S.O. são instalados aplicativos ou serviços que irão prover à rede serviços dos mais diversos. No entanto, com base nas boas práticas, é aconselhável que estes serviços sejam configurados de forma que forneçam à rede apenas o que é necessário, sendo descartada qualquer outra funcionalidade que não estará em uso. Isto é uma forma de diminuir a margem de risco do ambiente. Existe um serviço de rede onde, uma de suas finalidades, é transferir toda sua base de dados, neste caso conhecida como transferência de zona, para outro serviço existente para fins de redundância, o qual deve ser devidamente ajustado para evitar roubo de informações de facilitem o reconhecimento da rede por um invasor.

Com base no texto, a descrição acima refere-se ao serviço

Alternativas:
A) DNS
B) HTTPS
C) HTTP

D) FTP
E) SSH

Questão 2:
Para fazer uso da capacidade de processamento de um computador, é necessária a instalação de um sistema operacional, seja Windows ou Linux. Sobre este S.O. são instalados aplicativos ou serviços que irão prover à rede serviços dos mais diversos. No entanto, com base nas boas práticas, é aconselhável que estes serviços sejam configurados de forma que forneçam à rede apenas o que é necessário, sendo descartada qualquer outra funcionalidade que não estará em uso. Isto é uma forma de diminuir a margem de risco do ambiente.

Com base o texto, a técnica de configurar adequadamente um serviço e sistema operacional, diminuindo a margem de risco é conhecida por:

Alternativas:
A) Spoofing
B) NAT
C) hardening
D) Sniffing
E) Firewalling

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 13: Tema - 4. CONTRAMEDIDAS E HARDENING

3 Objetivos

- Entender os sistemas de segurança para redes sem fio, para que seja possível definir qual a melhor solução para os cenários de uso

- Conhecer os principais conceitos e funcionamento de ambiente IoT, para identificação de seus pontos frágeis com relação à segurança

4 Tópicos

4.4 SEGURANÇA EM REDES SEM FIO & INTERNET DAS COISAS

5 Procedimentos de ensino-aprendizagem

- Situação problema
Muito tempo se passou desde que a internet integrou o mundo, interligando pessoas através de seus dispositivos. No entanto, a evolução tecnológica trouxe os dispositivos inteligentes e, pouco mais adiante, a possibilidade de que estes equipamentos pudessem trocar dados entre si de forma autônoma, seja de forma parcial ou total. Esta integração inteligente entre dispositivos chamamos de IoT (Internet Of Things - internet da coisas). Neste ambiente equipamentos trocam informações uteis de controle e monitoramento entre si, sendo possível, por exemplo, que um dispositivo deixado em casa notifique o celular do proprietário da residência que uma luz foi deixada acessa, que um movimento foi percebido, a porta da geladeira foi deixada aberta, dentre outras utilidades. Esta interligação segue as premissas da mobilidade, possibilitanto que os dispositivos se comuniquem através de tecnologia sem fio. Contudo, este cenário aumenta a preocupação com a segurança e a legitimidade daqueles que tem acesso aos dados. Qual conhecimento voce tem a respeito desta tecnologia? Quais possibilidades e perigos aos quais ela expõe as pessoas?

- Metodologia
Com base em [1], sugere-se que o Docente introduza os alunos ao mundo IoT. Ainda com o auxílio de [2], apresentar aos alunosos requisitos para a existência de uma rede IoT e suas peculiaridades, sempre adordando o ponto de vista de segurança conforme [3]

- Verificação de Aprendizado
Com o uso da ferramenta [4] e mediação do Docente para posterior validação, formar grupos para construção fictícia de um ambiente residencial que contemple o máximo de dispositivos IoT possível, estimulando a imaginação da sala.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Comer, Douglas E. Redes de computadores e internet [recurso eletro^nico] / Douglas E. Comer ; traduc¸a~o: Jose´ Valdeni de Lima, Valter Roesler. 6. ed. Porto Alegre : Bookman, 2016. Páginas 8 e 498 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/cfi/1!/4/4@0.00:63.6

[2] Comer, Douglas E. Redes de computadores e internet [recurso eletro^nico] / Douglas E. Comer ; traduc¸a~o: Jose´ Valdeni de Lima, Valter Roesler. 6. ed. Porto Alegre : Bookman, 2016. Página 500 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/cfi/1!/4/4@0.00:63.6

[3] WRIGHTSON, Tyler. Segurança em Redes sem Fio: Guia do Iniciante. 1ª edição. Porto Alegre: Editora Bookman, 2013. Página 128 -
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601556
[4] Miro - Disponível em: https://miro.com/education-whiteboard/

8 Aprenda +

1) Segurança em IOT - Disponível em: https://youtu.be/JkzFkS5TsBE
2) IOT Privacidade e Segurança - Disponível em: https://youtu.be/zp0NOXv6THY

Atividade Autônoma Aura:

Questão 1:
As redes sem fio possibilitaram a mobilidade. Com uso desta tecnologia, dispositivos não precisam de cabos para trocar informações, pois estas trafegam pelo ar em forma de sinais de ondas de rádio em frequências que variam de países para países sendo, no brasil, as frequências de 2.4 Ghz e 5 Ghz. Contudo, por ser informação que é disseminada pelo ar em todas as direções, torna-se disponível para dispositivos terceiros que estejam dentro da área de alcance do sinal, colocando em risco o sigilo do que é transmitido. Para resolver este problema, utiliza-se mecanismo que torna inelegível conteúdo transmitido para terceiro não autorizado.

Com base no texto, o mecanismo que trata do sigilo dos dados trafegados em uma rede sem fio é

conhecido por:

Alternativas:
A) IoT
B) HTTPS
C) Twisted-pair
D) SSH
E) Criptografia

Questão 2:
Era tendência, e se realizou – os dispositivos trocarem dados diversos entre si de forma autônoma. Neste tipo de rede os dispositivos trocam informações das mais variadas, facilitando a vida do homem, pois o protege do risco de deixar a geladeira aberta, a TV ligada, o informa sobre movimentação dentro de sua casa quando estiver ausente, e muito mais.

Com base no texto e a tecnologia citada. Podemos falar que o conteúdo trata de:

Alternativas:
A) BYOD
B) IoT
C) Ethernet
D) Wifi
E) 5G

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 14: Tema - 5. RESPOSTA À INCIDENTES E RECUPERAÇÃO (DISASTER RECOVERY)

3 Objetivos

- Entender os diversos tipos de incidentes em ambientes tecnológicos, possibilitando elencar as principais soluções disponíveis para cada tipo de ocorrência

- Identificar as principais vulnerabilidades de sistemas computacionais, de forma a proceder com técnicas e sugestões de boas práticas para diminuição das margens de risco normalmente existentes

4 Tópicos

5.1 RESPOSTA À INCIDENTES
5.2 CORREÇÕES DE VULNERABILIDADES

5 Procedimentos de ensino-aprendizagem

- Situação problema
São muitos equipamentos e muito investimento para processar e armazenar tanta informação. Estas são usadas no dia-a-dia para fazer a empresa funcionar, garantindo renda para a empresa, funcionários e parceiros de negócios, além de viabilizar e agilizar o atendimento dos clientes. Alguns destes ambientes são responsáveis por cifras milionárias e, em um belo dia, tudo para, nada funciona. Cadê o arquivo que estava aqui? O contato do fornecedor sumiu. Cade os dados de faturamento da empresa? Como a empresa irá seguir adiante, se tudo desapareceu? Foi um hacker? Nem sempre! Uma chuva forte pode ser a responsável por inundar um datacenter mal posicionado. Quando falamos se cyber segurança, é necessário pensar em tudo (até na tomada de energia!), prever os piores cenários e agir para evitá-los desde a concepção inicial do projeto e durante toda sua existência. Voce sabia que existe um ciclo inacabável de melhoria continuada? Voce sabia que ela contempla a inserção e melhoria de resposta a incidentes e a verificação constante de vulnerabilidades existentes para que sejam corrigidas?

- Metodologia
Com base em [1], o Docente deve introduzir os alunos nos conceitos e diversos tipos diferentes de incidentes, bem como as ferramentas necessárias para sua detecção. Ainda utilizando [2] poderá entrar no campo das soluções a incidentes, o que inclui o saneamento de possíveis vulnerabilidades, conforme descrito em [3].

- Verificação de Aprendizado
A Atividade descrita abaixo computará 2.5 pontos para a AV2.
Utilizando [4], o Docente deve sugerir possíveis pesquisas em grupo por vulnerabilidades aos alunos, procedendo com a assistência quanto à tradução. Sugere-se a pesquisa pelos CVEs: CVE-2002-0283, CVE-2010-0816 e CVE-2020-15708. Por fim, sugere-se visita aos sites oficiais do ubuntu (https://ubuntu.com/security/cve) e da microsoft (https://msrc.microsoft.com/update-guide/vulnerability) onde os boletins de falhas dos sistemas e possiveis correções são divulgados. Os alunos desvem redigir um texto técnico sobre a pesquisa para, explicando de forma clara as vulnerabilidades e como as correções ocorreram, para entrega ao professor.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] BASTA Alfred. Segurança de Computadores e Testes de Invasão. 2ª edição. São Paulo: Editora Trilha, 2015. Página 309 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366

[2] BASTA Alfred. Segurança de Computadores e Testes de Invasão. 2ª edição. São Paulo: Editora Trilha, 2015. Página 321 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366

[3] McClure,Stuart. Hackers expostos: segredos e soluções para a seguranc¸a de redes / Stuart McClure, Joel Scambray, George Kurtz ; tradução: João Eduardo Nóbrega Tortello ; revisão técnica: Marcos A. Simplicio Jr., Charles Christian Miers. 7. ed. Dados eletrônicos. Porto Alegre : Bookman, 2014. - Página 669 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601426/cfi/19!/4/4@0.00:0.00

[4] "Programa CVE®" , Disponível em https://cve.mitre.org/cve/search_cve_list.html (Acessar usando o Chrome, e ativar a tradução para o Português)

8 Aprenda +

1) 5 Erros Que Todo Iniciante Comete - Segurança da Informação - Disponível em: https://youtu.be/wvKXB7eexWg
2) NOTIFICAÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA - Disponível em: https://youtu.be/S19Yy_xTWWM
3) Hardening básico de Linux - Disponível em :https://youtu.be/YZnkAWdXB4s

Atividade Autônoma Aura:

Questão 1:
Ambientes tecnológicos podem vir a ser bastante complexos, ou seja, composto por diversas soluções que exigem da equipe técnica de administração conhecimentos profundos dos mais variados para sua manutenção. Estes ambientes, por mais sofisticados e caros que possam ser, são susceptíveis a falhas e outros problemas das mais diversas origens, com soluções diferentes, sejam mais ou menos eficientes que as outras.

Com base no texto e com o objetivo de prover a melhor resposta aos mais diversos incidentes, é correto afirmar:

Alternativas:
A) Deve haver uma base de consolidação de problemas e soluções disponíveis para cada caso e acessível por todos do corpo técnico
B) Deve haver um profissional com conhecimento genérico disponível para combate imediato aos possíveis problemas
C) Os e-mails do suporte especializado devem estar disponíveis para abertura de chamado e atendimento imediato de um possível sinistro
D) Deve haver uma base de consolidação de problemas e soluções disponíveis para cada caso e acessível por todos da empresa
E) Para fins de otimização, inclusive financeira, sugere-se a contratação de apenas um profissional com alto conhecimento em toda tecnologia para suporte.

Questão 2:
A internet trouxe integração, o que inclui conhecimento técnico e ambientes de ajuda dos mais variados. Dentre estes existem aqueles onde empresas e comunidades de tecnologia fazem registros de vulnerabilidades encontradas em sistemas existentes, seja um aplicativo ou sistema operacional. Como forma de padronização e para facilitar a pesquisa e retorno do que é procurado na internet relacionado às vulnerabilidades, estas informações devem ter códigos de referência que iniciam com um prefixo, seguido do ano de detecção/descoberta da vulnerabilidade e seu número identificador.

Com base no texto acima, o prefixo utilizado para identificar as vulnerabilidades é:

Alternativas:
A) CSV
B) CVE
C) OWASP
D) PDF
E) RFC

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 15: Tema - 5. RESPOSTA À INCIDENTES E RECUPERAÇÃO (DISASTER RECOVERY)

3 Objetivos

- Entender a importância da ciência da forense computacional para solucionar crimes cibernéticos

- Compreender algumas técnicas de rastreamento, para identificação de criminosos e recolhimento de pistas

4 Tópicos

5.3 FORENSE COMPUTACIONAL

5 Procedimentos de ensino-aprendizagem

- Situação problema
Quando Gestão em Tecnologia da Informação é estudada, é praxe passar pelo assunto de princípios que norteiam a definição das boas práticas da área. Dentre estes, devemos lembrar do princípio da rastreabilidade, cujo conceito define que é prudente elencar quais atividades devem ter sua manipulação auditada, ou seja, quais devem ter registros das atividades executadas. Estes registros, bem como o nível de seu detalhamento depende de como a aplicação foi desenvolvida e da configuração definida por seu operador. O registro das atividades devem ser guardado, cada qual com períodos diferentes de quarentena, a depender da criticidade. Em outros casos, não há como ter logs de atividades, mas em muitos casos resquicios de ações permanecem imperceptíveis no ambiente, o que acaba servindo para o profissional que atua no ramo de investigação, conhecido como Perito Forense Computacional. Voce saberia informar onde este profissional é encontrado e em quai situações ele atua?

- Metodologia
Com base em [1], sugere-se que o Docente proceda com a apresentação do glossário utilizado na área forense computacional, em seguida abordando as funções de um processo de auditoria. Ainda com base em [2], trabalhar o assunto referente à implementação de sistemas de auditoria.

- Verificação de Aprendizado
Com a mediação do Docente e posterior validação, convidar os alunos pesquisarem serviços passíveis

de configuração de auditoria, tanto em ambientes Windows quanto Linux, bem como proceder com alguma implementação, caso viável.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] Stallings, William, William Stallings, Lawrie Brown - Segurança de computadores : princípios e práticas [tradução Arlete Simille Marques]. - 2. ed. - Rio de Janeiro : Elsevier, 2014. Página 520 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459/cfi/6/64!/4/2/14/6/2@0:0

[2] Stallings, William, William Stallings, Lawrie Brown - Segurança de computadores : princípios e práticas [tradução Arlete Simille Marques]. - 2. ed. - Rio de Janeiro : Elsevier, 2014. Página 528 - Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459/cfi/6/64!/4/2/18/2@0:16.1

8 Aprenda +

1) Computação Forense - O que faz um perito forense computacional - Disponível em:https://youtu.be/BocTBCT11WI
2) Hackers_ Computação Forense Ep. 9_20180714_2025 - Disponível em:https://youtu.be/UA3tvfrHbmE
3) Auditoria e Segurança da Informação Aula 01 - Disponível em:https://youtu.be/OE54j3BRQN0?t=267

Atividade Autônoma Aura:

Questão 1:
Gestão de tecnologia da informação é regulamentada com fundamento em diversos princípios, dentre eles o da rastreabilidade. Este, trata de que os sistemas devem ser desenvolvidos de forma a registrar suas atividades para uso futuro, seja para resolução de problemas, seja para auditoria.

Com base no texto acima, é comando do Windows que abre a interface de registro de atividades

Alternativas:
A) Services.msc
B) snifftool
C) msconfig
D) checkactivity
E) eventvwr

Questão 2:
O mundo evoluiu. A tecnologia tomou de assalto o cotidiano da humanidade e fez dela sua refém. Hoje em dia, quase tudo é digital. As ações, pensamentos e informações correm de um lado ao outro do globo terrestre em questões de milésimos de segundos. Dentre tudo que circula pelos meios de integração computacional, há aquilo fruto de ações erradas e/ou criminosas e podem ter resultados devastadores, o que indica que o ambiente tecnológico deve gerar informações de registro do que é feito para posterior análise.
Com base no texto acima e a respeito dos registros das atividades, é correto afirmar que o conteúdo de refere:

Alternativas:
A) À necessidade de utilização de linguagens de programação mais fáceis
B) Aos Logs
C) À necessidade de uso de firewall
D) À necessidade de uso de antivirus
E) À necessidade de uso de antispam

Plano de Aula

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Semana/Tema

Semana 16: Tema - 5. RESPOSTA À INCIDENTES E RECUPERAÇÃO (DISASTER RECOVERY)

3 Objetivos

- Compreender a importância de planos de contingência e contorno de sinistros, para recuperação de dados ou reestabelecimento de sistemas e operações em caso de sinistro

4 Tópicos

5.4 DISASTER RECOVERY PLAN

5 Procedimentos de ensino-aprendizagem

- Situação problema
Na área de tecnologia da informação, tida como uma área exata, tudo deve seguir previsão e planejamento para os mais diversos cenários. Fora isto, também são necessárias a documentação e descrição de procedimentos para o caso de sinistro, bem como a relação de interdependência entre soluções visto que, em ambientes de alta complexidade, é necessário atentar para a ordem de disponibilização das soluções, porque, nem sempre, uma solução pode ser ligada antes da outra, ou recuperada antes que outra já esteja completamente recuperada. Voce sabia que, em ambientes complexos, ligar uma solução antes de outra pode vir a causar corrompimento de dados importantes?

- Metodologia
Com base em [1] sugere-se que o Docente aborde o assunto relacionado aos controles de segurança necessários para a criação de um plano de recuperação. Utilizando [2] apresentar aos alunos algumas das etapas relacionadas ao plano de recuperação de desastres.

- Verificação de Aprendizado
Com o uso da ferramenta [3] e mediação do Docente para posterior validação, sugerir aos alunos que elenquem alguns ativos de datacenters, suas interligações e dependencias, posteriormente imaginando um cenário hipotético de pane elétrica total, onde será necessário religar os equipamentos, para que seja demonstrada a ordem correta de religação com a referida explicação. Opcionalmente, imaginar perda total de S.Os como controladores de domínios, servidores de arquivos, servidores FTP para que definam quais deles devem ter seus backups restaurados preferencialmente sobre os restantes.

6 Recursos didáticos

Laboratório de Programação de computadores e softwares, computador do docente com acesso à Internet e caixas de som, além de datashow. Sugere-se o software Virtualbox com Kali Linux 2021.1 ou superior, ubuntu linux 20.04 ou superior, Windows XP, 7 e 10 instalados e com snapshot de seu estado pós-instalação para posterior restauração. Para padronização do acesso, é aconselhável a definição de senha de administrador/root/aluno para todas VM a que é utilizada como senha padrão para o usuário aluno em cada unidade eduacional

7 Leitura específica

[1] STALLINGS, William. Segurança de Computadores - Princípios e Práticas. 2ª edição. Rio de Janeiro: Editora Elsevier, 2014. Página 465 -
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155459

[2] BASTA Alfred. Segurança de Computadores e Testes de Invasão. 2ª edição. São Paulo: Editora Trilha, 2015. Página 324 -
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366

[3] Miro - Disponível em: https://miro.com/education-whiteboard/

8 Aprenda +

1) DISASTER RECOVERY: o plano que vai RECUPERAR sua empresa de um DESASTRE! - Disponível em: https://youtu.be/abF5Rf352eM
2) Disaster Recovery Plan - Disponível em: https://youtu.be/TXlNvJXdMQo

Atividade Autônoma Aura:

Questão 1:
Quer diminuir a margem de erro de execução no trabalho? Siga os frameworks de boas práticas de gestão de tecnologia da informação! Eles são produto de reuniões e experiências de grandes profissionais e empresas renomadas da área e foram amplamente discutidos antes de serem aceitos e abordam vários temas. No tocante a disaster recovery plan, é correto afirmar

Alternativas:
A) O foco principal e único é o storage, onde estão armazenadas de fato todas as máquinas virtuais
B) O foco principal e único é o banco de dados, onde estão armazenadas de fato todas as informações
C) Deve procedimentos descritos e documentados antes do ambiente computacional entrar em atividade
D) Deve procedimentos descritos e documentados antes do ambiente computacional após entrar em atividade, o que permite conhecer bem o ambiente e seu real funcionamento.
E) Por segurança e facilidade de manutenção não é aconselhável haver múltiplos encaminhamentos físicos entre os ativos de rede, pois qualquer problema em um segmento dificulta sua identificação e resolução do sinistro para recuperação do ambiente.

Questão 2:
Muito há de ser investido em tecnologia e muitas são as tecnologias necessárias para satisfazer os

requisitos de segurança. Quando falamos em cyber segurança, não é correto pensar apenas em hackers e roubo de dados. É importante se lembrar que disponibilidade de informações e tecnologia também tem relação direta com segurança de dados, o que inclui o tempo que elas levam para serem novamente disponibilizadas em caso de sinistro.

Quando ocorre um incidente, como a perda de uma máquina virtual de um servidor, seja qual for o motivo, a maneira mais rápida de disponibilizá-la é:

Alternativas:
A) Restaurar seu último backup feito
B) Reiniciar a instalação de outra máquina virtual e chamar o suporte oficial para reinstalação da solução
C) Reiniciar a instalação de outra máquina virtual efetuar a reinstalação da solução sem espera pelo suporte oficial
D) Como solução de contorno para evitar a paralisação dos trabalhos, executar trabalho manual para posterior armazenamento em arquivo morto tradicional
E) Como solução de contorno para evitar a paralisação dos trabalhos, executar trabalho manual para posterior armazenamento em banco de dados quando o sistema retornar.