Curso Técnico em Desenvolvimento de Sistemas Online

SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

GEEaD - Grupo de Estudo de Educação a Distância

Centro de Educação Tecnológica Paula Souza

Expediente

GEEaD – CETEC
GOVERNO DO ESTADO DE SÃO PAULO
EIXO TECNOLÓGICO DE INFORMAÇÃO E COMUNICAÇÃO
CURSO TÉCNICO EM DESENVOLVIMENTO DE SISTEMAS
FUNDAMENTOS DE INFORMÁTICA

Autores:
Marcelo Fernando Iguchi
Eliana Cristina Nogueira Barion

Revisão Técnica:
Lilian Aparecida Bertini

Revisão Gramatical:
Juçara Maria Montenegro Simonsen Santos

Editoração e Diagramação:
Flávio Biazim

São Paulo – SP, 2019

APRESENTAÇÃO

Este material didático do Curso Técnico em Desenvolvimento de Sistemas modalidade EaD foi elaborado especialmente por professores do Centro Paula Souza para as Escolas Técnicas Estaduais – ETECs.

O material foi elaborado para servir de apoio aos estudos dos discentes para que estes atinjam as competências e as habilidades profissionais necessárias para a sua plena formação como Técnicos em Desenvolvimento de Sistemas.

Esperamos que este livro possa contribuir para uma melhor formação e apefeiçoamento dos futuros Técnicos.

AGENDA 7

TIPOS DE INVASÕES E VULNERABILIDADES

MERGULHANDO NO TEMA...

Você saberia dizer qual é a situação ideal para um crime perfeito na internet? Bem, adiantamos que esse cenário se divide em duas partes. De um lado, temos o usuário desprevenido de redes sociais, que adora compartilhar cada detalhe da sua vida nas mais diversas plataformas.

Do outro, o agente malicioso que se aproveita dessa disseminação voluntária de informações e utiliza esse material valioso para benefício próprio.

Imagem 02

Pode parecer uma historinha para assustar novatos na web, mas é exatamente assim que age um cibercriminoso que abre mão da chamada engenharia social. Com essa técnica simples, mas muito efetiva, é possível enganar os outros ao se aproveitar da confiança que o usuário tem nas plataformas sociais.

A partir daí, basta aplicar um golpe a fim de obter informações para acesso não autorizado a todo tipo de sistemas – de senhas de banco a contas de e-mail. O problema é que executivos e perfis corporativos são cada vez mais visados pelos atacantes, já que é nesse filão que os dados obtidos são mais sensíveis e, por consequência, valiosos.

Veja como funciona esse tipo de ataque...

O uso de personas virtuais para esse propósito é um recurso que ficou bastante popular entre cibercriminosos nos últimos tempos. Isso porque práticas clássicas de phishing, quando uma pessoa é “pescada” com um link malicioso enviado por e-mail, já não são mais tão eficazes quanto em outros tempos (embora ainda façam suas vítimas aqui e acolá).

Foi com base nisso que Mia Ash surgiu na web. A fotógrafa usava uma história envolvente para atrair funcionários de empresas dos setores de óleo e tecnologia. Apesar de parecer ser interessante em um primeiro momento, a moça era nada menos que a cria de um grupo chamado Cobalt Gypsy, conhecido por desenvolver golpes especialmente voltados para invasão de sistemas. E é exatamente assim que o golpe funciona.

Primeiro de tudo, os batedores escolhem suas vítimas: as favoritas são funcionários específicos de empresas, que geralmente possuem informações relevantes da corporação. Com o alvo na mira, os crackers entram em ação e, conversa vai, conversa vem, levam o contato para o WhatsApp.

Nesse canal, com todas as informações disponíveis (e entregues deliberadamente pelas presas) em mãos, os criminosos criam golpes, que posteriormente são aplicados por e-mail. Mia poderia muito bem ser alguém de carne e osso, mas era apenas uma ferramenta social que dava acesso a usuários, senhas e muitos dados sigilosos.

Você sabe o que podemos aprender com isso?

Basicamente, que não se deve confiar cegamente nas redes sociais. Partimos do pressuposto de que todos que estão na internet, conectados via LinkedIn, Facebook ou qualquer outra plataforma do tipo, são reais. Por conta disso, criamos uma confiança que nem sempre é real.

Em entrevista ao site Inc., o especialista em inteligência de ameaças da PhishLabs, Crane Hassold, observa que "esta confiança implícita pode tornar os ataques de phishing de redes sociais mais bem-sucedidos, especialmente quando associado a um ator sofisticado que utiliza uma estratégia de 'longo prazo' para construir um relacionamento com uma vítima antes de explorá-la".

E, sim, crackers podem se empenhar bastante para conquistar a vítima, se o resultado da investida for lucrativo o suficiente (#ROI). Mia, por exemplo, poderia passar semanas enaltecendo seu alvo. "Vimos que eles (os membros do Cobalt Gypsy) demonstram um alto grau de criatividade e persistência nos ataques", diz Allison Wikoff, pesquisador sênior da Dell SecureWorks Counter Threat Unit.

No caso de Mia Ash, quando a vítima já estava pronta para o golpe final, ela recebia um formulário que solicitava respostas a uma pesquisa fotográfica. Até aí, nada demais, não é mesmo? O que a pessoa não sabia é que, na verdade, ela estava baixando um cavalo de troia que garantiria acesso remoto e irrestrito ao sistema. Missão cumprida!

Moral da história: não confie em estranhos, como diria qualquer mamãe pelo globo. Sendo assim, cuidado com quem você se relaciona nas redes. Afinal, do outro lado da conexão pode haver uma Mia Ash pronta para a emboscada. Pode-se notar que um contato inocente por e-mail ou rede social tem a chance de comprometer toda a segurança de uma empresa ou equipamento, por isso devemos mergulhar no tema para sabermos mais sobre ataques e como prepararmos as redes de computadores e os próprios equipamentos de ataques cibernéticos.

Fonte: https://www.thebrief.com.br/mercado/119078-engenharia-social-arma-hackers-invadir-empresa.htm. Acessado em 28/11/18.

A história contada é um caso de Engenharia Social. Na engenharia social são utilizadas técnicas que tentam convencer o alvo do golpe utilizando técnicas psicológicas a fornecerem os dados confidenciais necessários a aplicação do golpe ou a realizar ações como envio de e-mails, cópia de arquivos sigilosos ou transferências de fundos. O alvo primário é o ser humano. No artigo anterior, o tradicional phishing scan foi substituído pela engenharia social para instalar um Cavalo de Tróia no computador da vítima.

Outro exemplo de Engenharia Social muito comum aqui no Brasil é quando o criminoso liga para a vítima falando ser do banco na qual ela tem conta alegando que o seu cartão está com um problema qualquer e para a substituição é necessário que a vítima envie o cartão com a senha de volta para o banco por intermédio de um motoboy.

Imagem 03

Assim que o cartão é entregue ao criminoso, esse passa a ter acesso à conta bancária, podendo realizar compras e saques em nome da vítima. Todos sabemos que nunca devemos entregar um cartão ou nome de usuário de uma conta em conjunto com a senha para nenhuma pessoa. Contudo os golpistas são tão convincentes nas histórias que contam que muitas pessoas acabam caindo nos golpes da engenharia social.

Por esse exemplo percebe-se que a Engenharia Social não está presente somente nos meios virtuais e eletrônicos. Ela está presente no ambiente real também. Por isso, sempre que alguém pedir uma informação por meios não usuais ou conte alguma história que soe estranha, cheque primeiro com a pessoa ou empresa solicitante, por um meio que seja comprovadamente seguro, se a solicitação é real.

Ataques de Negação de Serviço

Os ataques de negação de serviço (Denial of Service – DoS) geralmente se concentram tipicamente em servidores da Internet. Ele são feitos com o intuito de congestionar os meios de comunicação até o servidor ou sobrecarregar o alvo para que a sua resposta fique lenta por consumir recursos de sistema (memória RAM, uso do processador etc.), forçando a sua reinicialização, fazendo com que o serviço oferecido não possa mais ser fornecido.

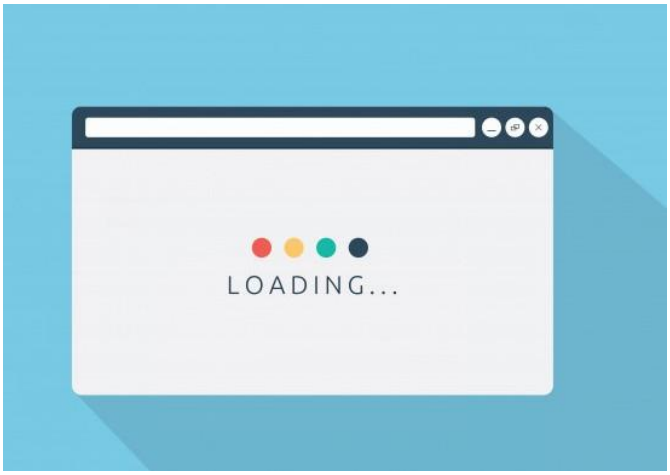


Imagem 04

O ataque do tipo DoS pode ser feito explorando-se falhas no protocolo TCP/IP (Transmission Control Protocol/ Internet Protocol), sendo possível ocorrer em qualquer computador que o utilize. Veja um exemplo de ataque do tipo DoS:

Na época em que a grande maioria dos usuários se conectava na internet por meio de uma conexão discada de baixa velocidade (56kbps) e um atacante utilizava uma conexão de internet mais veloz (1mbps, por exemplo) de uma empresa ou centro acadêmico, conseguia disparar centenas de pacotes tendo como alvo o computador da conexão discada, essa facilmente ficaria sobrecarregada ocorrendo uma negação de serviço.

Atualmente os ataques DoS evoluíram para DDoS (Distributed Denial of Service – Negação de Serviço Distribuído). Em um ataque DDoS centenas ou até milhares de computadores, chamados de computadores zumbis, formam um “exército” com o intuito de atacar um único alvo. Esses zumbis são comandados por um mestre que envia as ordens da investida.

O ataque DDoS funciona da seguinte forma: primeiro um worm ou um phishing scan contamina uma máquina tornando-a um zumbi respondendo aos comandos enviados pelo mestre. Segundo, quando um ataque é iniciado o mestre envia um comando que programa todos os zumbis para atacarem um mesmo alvo, em geral um servidor, na mesma data e hora. Os servidores são dimensionados para trabalhar com um certo número de requisições simultâneas. Quando o ataque DDoS é iniciado o servidor atacado recebe um número de solicitações de serviços proveniente da rede zumbi muito superior à sua capacidade de trabalho causando em um primeiro momento uma lentidão nas respostas, podendo evoluir para uma reinicialização do sistema ou travamento completo.

Quando o servidor atacado trava ou reinicia, temos a negação do serviço, pois ao cliente realizar alguma requisição o servidor não responde. Um exemplo de vírus que exploram rotinas de negação de serviço é o MyDoom.

A prevenção de ataques DoS e DDoS é muito complicada. Primeiro porque existem várias ferramentas e técnicas diferentes para os ataques. Isso permite disfarçar o pacote transmitido pela rede que contém ataque em um pacote de rede legítimo que trafega no servidor, dificultando a identificação por firewalls e softwares de monitoramento. Uma saída seria aumentar a capacidade dos servidores, mas isso nem sempre é viável economicamente.

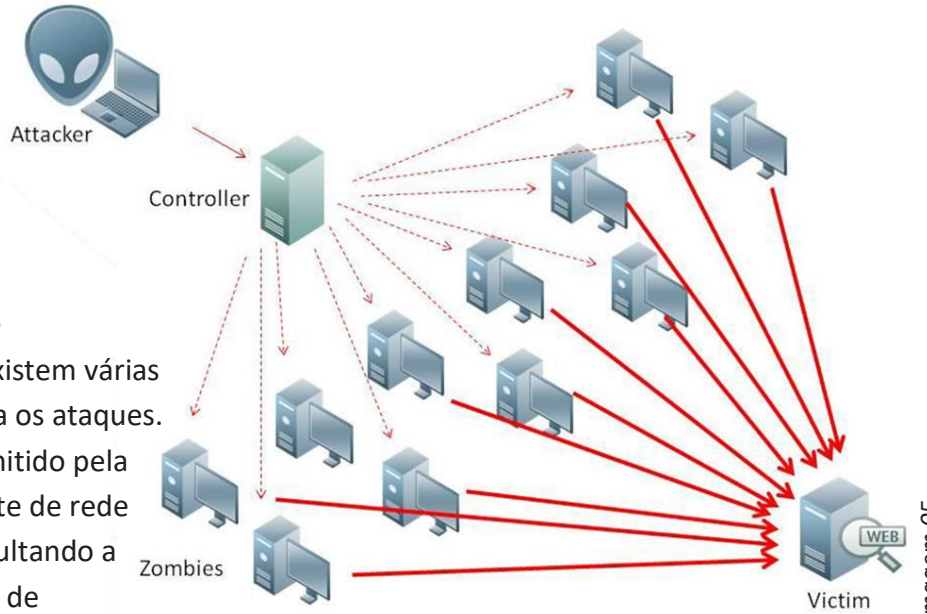


Imagem 05

Quer saber mais sobre Negação de Serviço? Acesse "Denial of Service – Negação de serviço". Link: https://www.gta.ufrj.br/grad/06_1/dos/index.html -acessado em 02/12/2018.

SQL Injection

Antes de falar de SQL Injection, vamos recapitular brevemente que os Bancos de Dados Relacionais são de extrema importância no mundo atual pois estes armazenam os dados de forma organizadas de pessoas, produtos, estoques, vendedores, compras, vendas etc. Os bancos de dados utilizam uma linguagem chamada de SQL para a criação, consulta, exclusão ou alteração dos dados nele contidos.

É exatamente nesse ponto que um ataque de SQL Injection age! Ele funciona por meio de uma inserção ou manipulação (injection) de uma consulta SQL que é enviada diretamente a um banco de dados quando não existe uma validação dos dados antes da realização desta consulta.

Exemplificando: Quando acessamos o Ambiente Virtual de Aprendizagem do curso, a primeira informação solicitada é o nome do usuário e senha. Que pode gerar um comando SQL da seguinte forma:

```
Select * from usuario where login = 'user' and password = 'senha';
```

Onde: user é o usuário digitado pelo cliente e senha é a senha digitada.

O problema começa se o sistema não realiza nenhuma verificação nos dados que o usuário digitou, pois se o site for mal intencionado, pode realizar uma Injection SQL ao substituir o campo user por admin'-- e uma senha qualquer.

```
Select * from usuario where login = 'admin'-- and password = 'senha';
```

Esse comando faria com que o banco de dados (BD) conectasse o usuário com a login admin, geralmente utilizado por administradores e tenha acesso privilegiado para a utilização do BD. Mas aí você pergunta: "mesmo sem saber a senha somente com o nome de usuário (login)?"

A resposta é sim! Pois o comando "--" faz com que o SGBD (Sistema Gerenciador de Banco de Dados) ignore o resto do comando, no exemplo ignorando a senha. Agora, imagine um criminoso com privilégio de acesso de um administrador, podendo modificar dados ou até mesmo apagar tabelas do Banco de Dados! Seria um estrago de tamanho incalculável, tanto do ponto de vista financeiro quanto da reputação de uma empresa.

Para prevenir os Injections SQL é fundamental que seja realizado um tratamento nos dados inseridos no sistema: parametrizar as consultas, utilizar "stored procedures" em SQL, limitar os privilégios no acesso ao BD, seja por programas desenvolvidos ou por interfaces WEB de modo a garantir que os comandos SQL executados pelo SGBD sejam seguros.

Leia o artigo: "Como evitar SQL Injection". Acesse "Evitando SQL Injection em aplicações PHP". Link: https://www.devmedia.com.br/evitando-sql-injection-em-aplicacoes-php/27804 - acessado em 02/12/2018.

Prevenção de ataques e invasões

Nessas agendas estudamos sobre as várias vulnerabilidades que computadores, dispositivos móveis e equipamentos de Internet das Coisas (IoT) estão sujeitos. Na agenda anterior vimos algumas dicas de proteção para equipamentos pessoais e atitudes comportamentais para não ser infectados por pragas virtuais. Mas, e no ambiente empresarial? Quais medidas devem ser tomadas para evitar aborrecimentos e perdas? A resposta, infelizmente não é simples. Temos que nos precaver com várias medidas. A seguir são apresentadas algumas delas:

Testes de Varredura e análise

Uma das primeiras medidas de segurança que devem ser feitas em uma rede é a varredura e a análise do sistema como um todo para identificar as vulnerabilidades do sistema.

Imagem 06

Depois de instalar os firewalls, sejam eles por software ou por hardware, instalar os antivírus nos computadores e servidores deve-se utilizar programas específicos chamados scanners para a varredura de vulnerabilidade na rede. Esses scanners analisarão os softwares instalados, a infraestrutura e a políticas de segurança em busca de vulnerabilidades, realizando uma classificação por nível como baixo, médio e alto risco.

Como exemplos de programas que realizam a varredura de vulnerabilidades temos o netsparker, aconetix, openvas, Nexpose e Wireshark.

De acordo com o resultado do teste de varredura, o analista de TI realizará a análise dos dados para sanar as vulnerabilidades detectadas priorizando as mais críticas (alto risco).

Teste de Penetração e vulnerabilidades

Contudo, dependendo do tamanho da empresa ou organização e do ramo de atividade do negócio, somente a varredura e a análise podem não ser suficientes. Isso porque uma varredura somente identifica as vulnerabilidades do sistema. Em um teste de penetração ou pentest (penetration test), além da identificação da vulnerabilidade os testadores tentam explorá-la, ou seja, tentam invadir o sistema avaliando os danos que essa invasão bem sucedida pode causar na empresa, podendo inclusive mensurar isso financeiramente com os sistemas que foram afetados ou paralisados. Quase sempre são contratadas empresas terceirizadas para realizar um pentest.

Um pentest pode ser classificado de três formas:

- White-box: quando as informações sobre a infraestrutura da empresa são fornecidas, facilitando e otimizando a busca por vulnerabilidades;
- Black-box: quando nenhum tipo de informação é fornecido e os testes são conduzidos de fora do ambiente da empresa;
- Grey-box: quando, de dentro da empresa, o testador tenta invadir outros ambientes corporativos internos. É uma opção interessante para testar e auditar processos de segurança internos.

O processo de um pentest, em geral, conta com os seguintes passos:

1) Footprint

É a fase inicial de um pentest onde são pesquisa das informações como endereços de IP, informações de colaboradores das empresas, endereços de correio eletrônico, versões dos softwares ativos na rede, sistemas operacionais utilizados (finger- print) e números de telefones. Muitas dessas informações podem ser descobertas em serviços de busca na internet como Google, Whois etc.

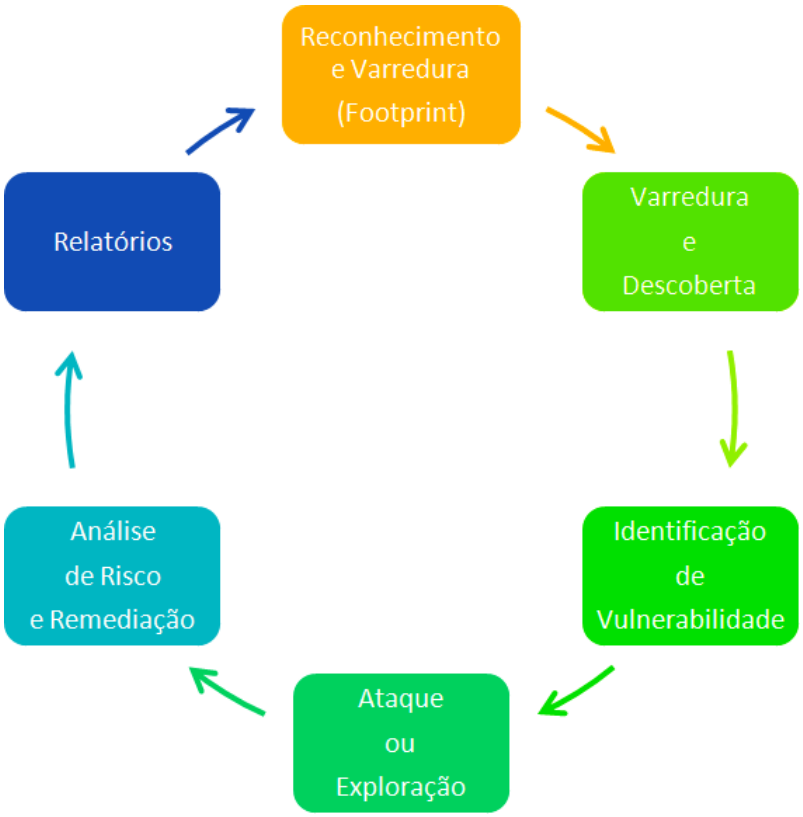


Imagem 07

2) Varredura e Descoberta

Nessa fase, o pentester tem um contato direto com o sistema a ser testado utilizando ferramentas de escaneamento de rede como Nmap e ZenMap para identificar portas, serviços ativos, ranges de IP etc.

3) Identificação de Vulnerabilidades

Com a varredura realizada as ferramentas de escaneamento de vulnerabilidades são usadas para detectar possíveis brechas no sistema como programas de segurança mal configurados ou atualizações de falhas de segurança conhecidas em programas não realizadas.

4) Ataque ou Exploração

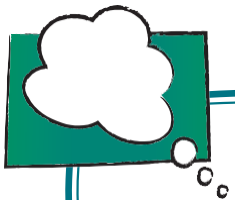
Com as informações obtidas nas fases anteriores, o pentester tentará invadir o sistema por meio das explorações de brechas de segurança conhecidas ou identificadas na fase anterior, sempre tentando passar despercebido pelos administradores de sistema ocultando os seus rastros.

5) Análise de Risco e Remediação

Após a invasão, os riscos são analisados e são recomendadas as atualizações e/ou modificações nos sistemas, com a devida documentação para o contratante.

6) Relatórios

Por último, após todo o teste de invasão do sistema, é elaborado um relatório com a metodologia utilizada, as vulnerabilidades encontradas, os ataques realizados e as correções necessárias.



Para quem está interessado na área de segurança da informação, algumas indicações para iniciar os estudos: estude profundamente sobre redes de comunicação de dados, protocolos de transferência de informações e sistemas operacionais. Para teste de sistemas, em geral, são utilizadas distribuições Linux. Uma das distros mais indicadas é o Kali Linux que contém diversas ferramentas para testes de segurança.

EXERCITANDO E APRIMORANDO

1. Defina Engenharia Social.
2. Como funciona um ataque do tipo DDoS?
3. O que é uma SQL Injection?
4. Uma Varredura e análise de um sistema é o mesmo que realizar um Pentest?
5. O que é Footprint? E Fingerprint?

Respostas:

1. A Engenharia social pode ser definida como um conjunto de métodos psicológicos de persuasão ao usuário, muitas vezes contando com a ingenuidade deste, para ganhar a sua confiança fazendo com que a vítima revele informações sensíveis para serem utilizadas em um ataque aos sistemas de uma empresa.

2. Um ataque do tipo DDoS funciona com centenas ou milhares computadores de uma rede "zumbi" infectados com um malware controlado pelo criminoso no qual em uma mesma data e hora atacam um único alvo com o intuito de tentar derrubar o serviço oferecido por este servidor causando a negação de serviço.

3. Podemos definir uma SQL Injection como a inserção de um código em linguagem SQL em uma query de um programa ou aplicação WEB com o intuito de obter dados sigilosos ou ganhar acesso não autorizado para a manipulação de um Banco de Dados.

4. Uma varredura ou análise do sistema, como o próprio nome denota somente realiza uma identificação das vulnerabilidades do sistema testado para que sejam corrigidas. Já um pentest além da execução da varredura e análise também realiza testes de invasão efetiva do sistema indicando as brechas para a intrusão do sistema.

5. Footprint consiste na análise inicial de um sistema alvo com a intenção de obter dados de forma segura sem ser detectado. Essa investigação inicial inclui pesquisas em mecanismos de busca, consultas ao Whois, visitas as páginas da internet da empresa, saber os domínios e endereços de IP, informações sobre os funcionários da empresa, endereços de e-mail etc.

O Fingerprint é uma parte do footprint que identifica o sistema operacional e demais softwares do alvo. Para isso são utilizadas ferramentas de scanner de rede.

Fontes Imagéticas:

Imagens de 1 a 4 - freepik.com

Imagem 05: DDoS attack - Pixabay - Disponível https://upload.wikimedia.org/wikipedia/commons/9/93/Ddos-attack-ex.png - Acessado em 28/11/2018.

Imagem 06: freepik.com

Imagem 07: Fases do pentest – Arquivo do GEEaD.