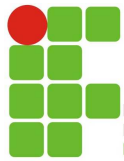
Segurança de Redes

Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 03
Ataques de Segurança da Informação (Continuação)



"Sempre que houver alternativas, tenha cuidado. Não opte pelo conveniente, pelo confortável, pelo respeitável, pelo socialmente aceitável, pelo honroso. Opte pelo que faz o seu coração vibrar. Opte pelo que gostaria de fazer, apesar de todas as consequências." (Osho)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

O que Aprenderemos?

- Aprender os passos realizados para um ataque específico (equipamento ou rede):
  - Levantamento de Informações;
  - Exploração de Vulnerabilidade;
  - Ataques diversos.

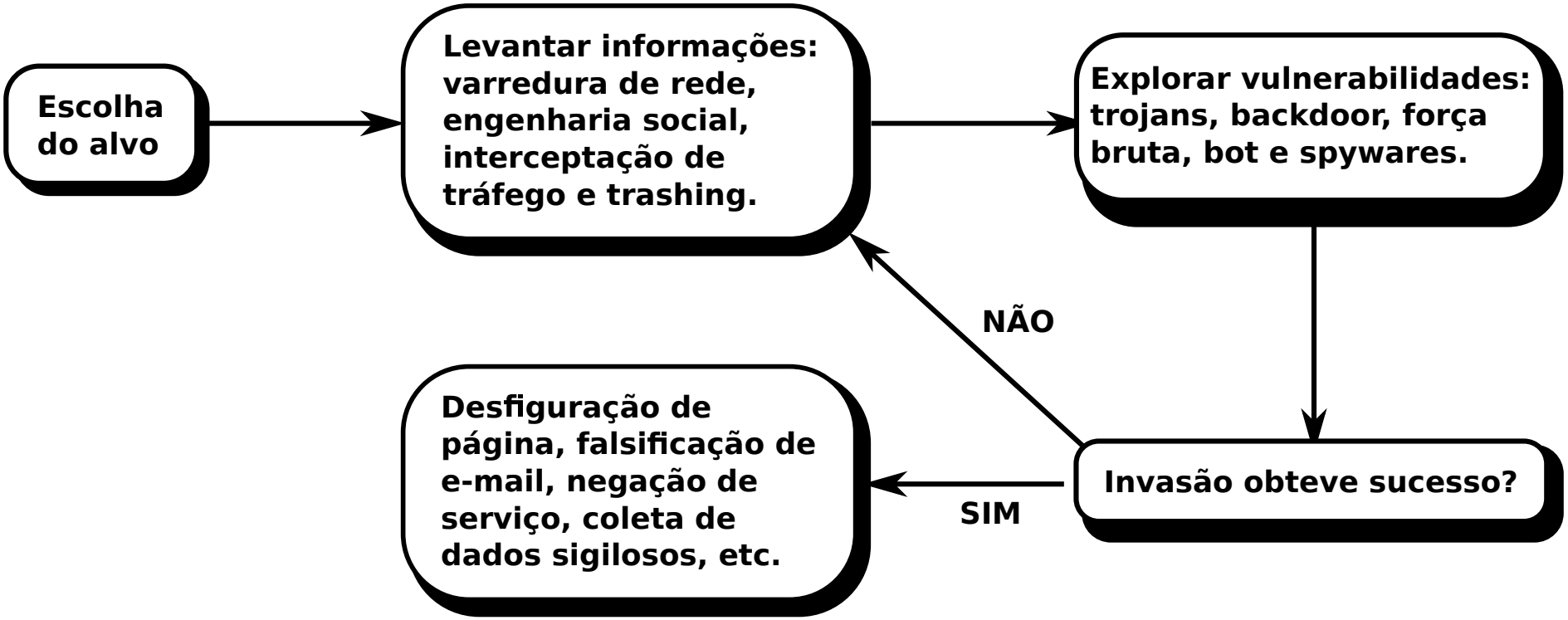
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ataques Específicos

Na aula anterior conhecemos os *malwares* que são códigos maliciosos utilizados para ataques. Entretanto, eles normalmente são desenvolvidos para atacar a quantidade máxima de pessoas possíveis. Os ataques que iremos conhecer agora são voltados, normalmente, para uma instituição ou indivíduo específico. Normalmente, eles são realizados em conjunto para ter uma maior efetividade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataques Específicos



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Levantar Informações - Varredura em Rede (*Scan*)

É uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados, sistemas operacionais e programas instalados. O principal *software* utilizado neste fase é o Nmap. Com base nas informações coletadas é possível associar vulnerabilidades aos computadores ativos detectados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Levantar Informações - Engenharia Social

Engenharia social é uma técnica empregada por criminosos virtuais para, através de manipulação psicológica, induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Além disso, os hackers podem tentar explorar a falta de conhecimento do usuário.

O elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Levantar Informações - Engenharia Social

Normalmente, a engenharia Social explora vulnerabilidades emocionais da vítima e usa como isca assuntos atuais, promoções ou até mesmo falsas premiações. Por exemplo, e-mails de *phishing* tentam convencer os usuários de que são, de fato, de fontes legítimas, na esperança de conseguir obter qualquer dado pessoal ou corporativos. Os e-mails também podem conter anexos cheios de *malwares*. A mensagem normalmente contém palavras atraentes ou intrigantes, que motivam o usuário desavisado a clicar no link.

Por exemplo, um cracker pode frequentar a praça de alimentação de um edifício corporativo e bisbilhotar os usuários, tentando coletar dados como o nome, datas importantes, relações familiares e o cargo. Após adquirir estas informações, o hacker pode depois de se disfarçar de usuários legítimos para o pessoal do suporte de TI.

Levantar Informações - Engenharia Social

Em alguns casos, os atacantes tentam reduzir a probabilidade de as vítimas denunciarem uma infecção, por exemplo, criando páginas/e-mails com ofertas para baixar um gerador de números de cartão de crédito, método para aumentar o saldo da conta on-line da vítima, proposta de emprego para pessoas empregadas ou sites de relacionamentos para pessoas casadas. Nesses casos, quando se descobre que passou informações, a vítima não quer divulgar suas intenções. Portanto, é provável que ela não denuncie a infecção para as autoridades legais.

A proteção contra a engenharia social começa com o treinamento. Os usuários devem ser condicionados a nunca clicar em links suspeitos e a sempre proteger suas credenciais de login, seja em casa ou no trabalho.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Levantar Informações - Interceptação de tráfego (*Sniffing*)

É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*, por exemplo Wireshark. Atacantes podem capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Levantar Informações - *Trashing*

Também chamado de dumpsterdiving, nele os atacantes procuram informações nos lixos das empresas ou das casas das pessoas a serem atacadas, como por exemplo, nomes de usuários e senhas, informações pessoais e confidenciais.Também são buscadas outras informações, como: organogramas, impressões de códigos fonte, inventário de *hardware*, topologia.

Esta técnica é considerada legal, uma vez que estas informações foram recuperadas do lixo por terem sido consideradas sem qualquer valor pela empresa ou pessoa alvo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Explorar Vulnerabilidade - Força bruta

Consiste em adivinhar, por tentativa e erro, com o auxílio de *software* específicos, um nome de usuário e senha. Desta forma, executar programas e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Explorar Vulnerabilidade - Força bruta

As tentativas de adivinhação costumam ser baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0" ';
- sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Explorar Vulnerabilidade - Ataque Físico

Este tipo de ataque é obtido quando um atacante consegue ter acesso físico ao seu ambiente de rede e obtêm alguma informação valiosa ou danifica equipamentos.

Para se proteger deste tipo de ataque você deve impedir, restringir ou controlar o acesso a determinados ambientes de sua rede. Uma forma de garantir isso é através do uso de crachás de identificação, documentos de identidade, câmeras de vídeo, etc.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataque de Falsificação de e-mail (*E-mail spoofing*)

É uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos e envio de spam. Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataque de Desfiguração de página (*Defacement*)

É uma técnica que consiste em alterar o conteúdo da página Web de um site. As principais formas que um atacante, pode utilizar para desfigurar uma página Web são:

- explorar erros da aplicação Web;
- explorar vulnerabilidades do servidor de aplicação Web;
- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;
- invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;
- furtar senhas de acesso à interface Web usada para administração remota.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

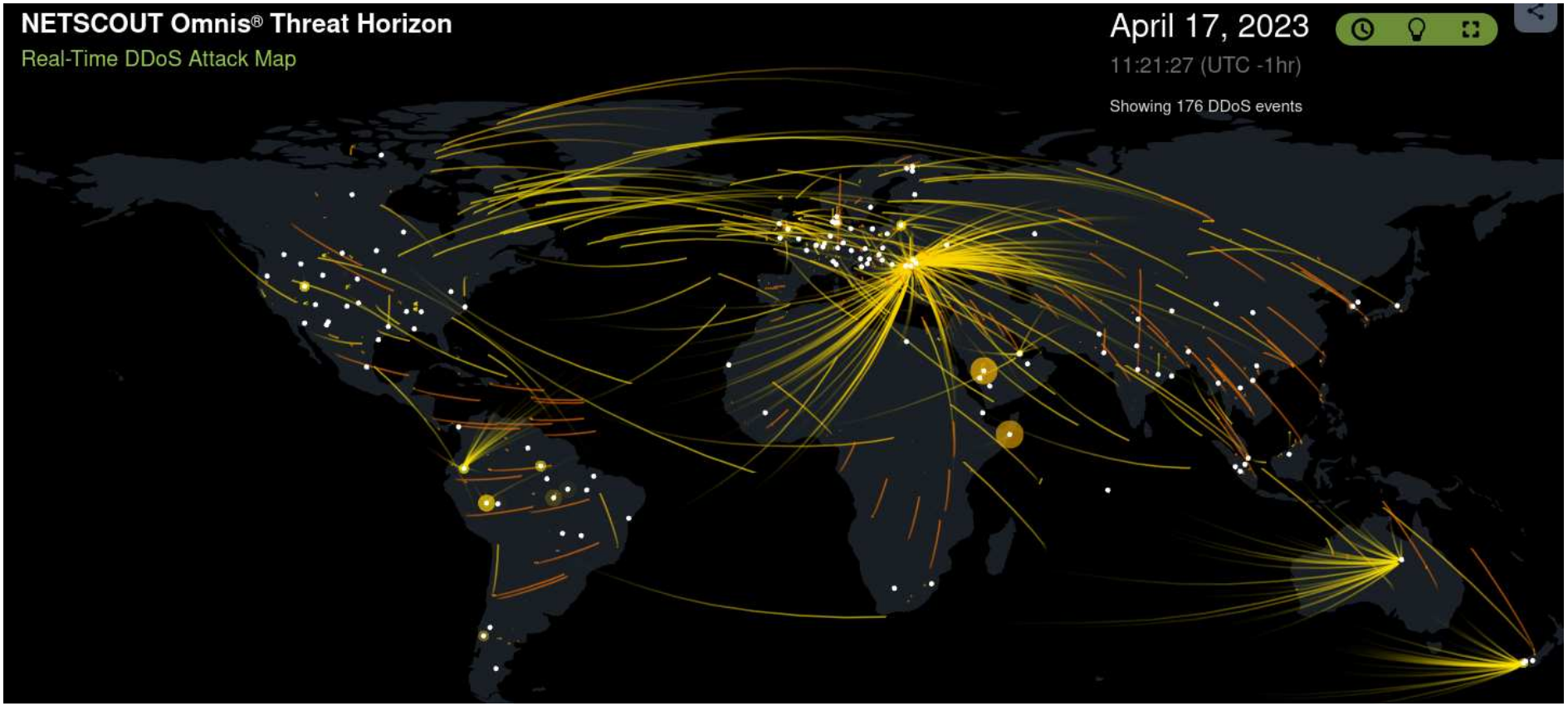
Ataque de Negação de serviço (DoS e DDoS)

Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataque de Negação de serviço (DoS e DDoS)



`https://horizon.netscout.com/`

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE