Princípios de Segurança da Informação
Cibersegurança

ATAQUES CIBERNÉTICOS

Aula 09

Professor Renato Oliveira

ATAQUES CIBERNÉTICOS

- Ataques cibernéticos são investidas criminosas de terceiros que visam comprometer e "derrubar" sistemas e sites, roubar informações confidenciais, alterar integridade de informações, desativar sistemas de inteligência militar (intenção política), etc.

- Os ataques cibernéticos são realizados por indivíduos ou organizações com intenções políticas, criminosas ou pessoais de destruir ou obter acesso a informações confidenciais.

- Alguns atacantes podem visar apenas o caos e "se aparecer" no meio do cibercrime.

ATAQUES CIBERNÉTICOS SÃO CRIMES!!!!

ATAQUES CIBERNÉTICOS

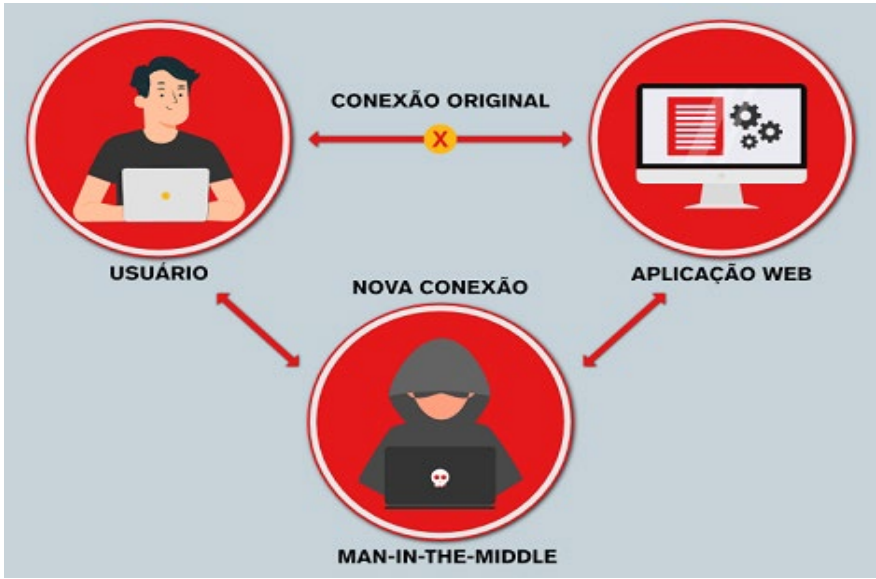
Prefeitura do Rio depois do ataque hacker

ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”

- É um ataque caracterizado pela presença de um terceiro elemento escondido, oculto, entre a comunicação de outros dois computadores (ou celulares, roteadores, etc).

- O cibercriminoso desvia o fluxo de informações entre duas conexões e dessa forma pode acessar e filtrar pacotes de rede, alterá-los ou redirecioná-los.



ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”

- Neste ataque o computador do criminoso se faz passar pelo gateway da vítima (roteador, como por exemplo o roteador de nosso provedor de internet).
- O atacante faz isso através do processo de "envenenamento" da tabela ARP (que como sabemos registra o IP e o MAC Address das placas de rede presentes na mesma rede).
- Dessa forma o atacante "engana" o tráfego de rede e toda a comunicação que deveria sair para a internet, passa primeiro pelo computador do criminoso que pode filtrar e acessar essa informação.
- Esse ataque é feito através de ferramentas específicas para isso, tais como a combinação do Ettercap e WireShark https://www.ettercap-project.org/

ATAQUES INTERNOS

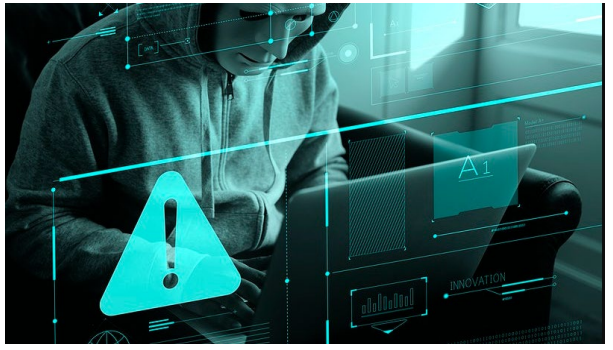
Man-in-the-Middle – “Homem no meio”

```
>arp -a

Interface: 192.168.15.17 --- 0xb
  Internet Address      Physical Address      Type
  192.168.15.1          [redacted]-75-78      dynamic
  192.168.15.16         [redacted]-7e-1e      dynamic
  192.168.15.255        [redacted]-ff-ff      static
  224.0.0.2             [redacted]-00-02      static
  224.0.0.22            [redacted]-00-16      static
  224.0.0.251           [redacted]-00-fb      static
  224.0.0.252           [redacted]-00-fc      static
  239.255.255.250       [redacted]-ff-fa      static
  255.255.255.255       [redacted]-ff-ff      static

Interface: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.56.255        [redacted]-ff-ff      static
  224.0.0.2             [redacted]-00-02      static
  224.0.0.22            [redacted]-00-16      static
  224.0.0.251           [redacted]-00-fb      static
  224.0.0.252           [redacted]-00-fc      static
  239.255.255.250       [redacted]-ff-fa      static
```


Imagem 1. Listagem da tabela ARP – Windows.

ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”



```
>arp -a

Interface: 192.168.15.17 --- 0xb
  Internet Address      Physical Address      Type
  192.168.15.1          [redacted]-7e-1e      dynamic
  192.168.15.16         [redacted]-7e-1e      dynamic
  192.168.15.255        [redacted]-ff-ff      static
  224.0.0.2             [redacted]-00-02      static
  224.0.0.22            [redacted]-00-16      static
  224.0.0.251           [redacted]-00-fb      static
  224.0.0.252           [redacted]-00-fc      static
  239.255.255.250       [redacted]-ff-fa      static
  255.255.255.255       [redacted]-ff-ff      static

Interface: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.56.255        [redacted]-ff-ff      static
  224.0.0.2             [redacted]-00-02      static
  224.0.0.22            [redacted]-00-16      static
  224.0.0.251           [redacted]-00-fb      static
  224.0.0.252           [redacted]-00-fc      static
  239.255.255.250       [redacted]-ff-fa      static
```


Imagem 2. Listagem da tabela ARP durante o ataque de poisoning – Windows.

ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”

- Através de ferramentas mais sofisticadas, como por exemplo o BetterCap (www.bettercap.org), os ciber criminosos podem:
  - Tirar screenshots do que a vítima vê de tempos em tempos.
  - Inserir na página acessada um JavaScript criado pelo atacante.
  - Executar processos que tentem abrir o tráfego criptografado HTTPS.
  - Inserir um keylogger que capture tudo que a vítima digitar.

ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”

Prevenção

- Evitar (se possível) utilização de redes públicas (shoppings, terminais urbanos, ônibus, etc). Esse tipo de ataque é mais bem sucedido em redes Wifi. Se for necessário acessar uma rede Wifi pública, evitar fazer logins, compras e autenticações durante o acesso.
- Instalar apenas softwares de fontes conhecidas
- Antivírus
- Segregar redes em sub redes
- Configurar de forma correta roteadores e firewalls

ATAQUES INTERNOS

Man-in-the-Middle – “Homem no meio”

A evolução das ameaças virtuais

ATAQUES INTERNOS

Keyboard loggin

- Um keylogger, também conhecido como keystroke logging, pode ser um software ou dispositivo que registra e armazena todos as teclas pressionadas por um usuário em um computador ou dispositivo móvel.

- As informações obtidas por um keylogger podem ser armazenadas em um arquivo de texto ou na memória do computador, para posteriormente serem enviadas ao servidor de um atacante de diferentes formas.

- Embora existam programas desse tipo para usos legítimos, quando são usados para fins maliciosos e/ou sem o consentimento do usuário, são considerados um tipo de malware dentro da categoria de spyware.

ATAQUES INTERNOS

Keyboard loggin

- Nestes casos, a partir do uso de um keylogger para espionar as conversas, o atacante usará o programa para roubar informações sigilosas, como credenciais para acessar contas através do home banking, conversas de chat, mensagens de e-mail, entre outros tipos de informação pessoal que o usuário inseriu usando o dispositivo comprometido.

- Atualmente os keyloggers estão mais avançados, adicionando além da capacidade de gravar pressionamento de teclas, a capacidade de controlar a câmera do computador da vítima, fazer prints da tela, obter informações da área de transferência (CTRL + C em memória) entre outras opções. Alguns keyloggers também têm a capacidade de gravar chamadas de voz e controlar o microfone do dispositivo.

ATAQUES INTERNOS

Keyboard loggin

access.log - Notepad

File Edit Format View Help

```
2019-07-09 16:06:30,045› New Tab - Google Chrome› Key.caps_lock
2019-07-09 16:06:30,361› New Tab - Google Chrome› 't'
2019-07-09 16:06:30,523› New Tab - Google Chrome› 'h'
2019-07-09 16:06:30,571› New Tab - Google Chrome› 'i'
2019-07-09 16:06:30,750› New Tab - Google Chrome› 's'
2019-07-09 16:06:32,439› New Tab - Google Chrome› Key.space
2019-07-09 16:06:35,576› YouTube - Google Chrome› 'i'
2019-07-09 16:06:35,733› YouTube - Google Chrome› 's'
2019-07-09 16:06:35,813› YouTube - Google Chrome› Key.space
2019-07-09 16:06:36,220› YouTube - Google Chrome› 'a'
2019-07-09 16:06:36,522› YouTube - Google Chrome› Key.space
2019-07-09 16:06:39,713› Facebook - Google Chrome› 'k'
2019-07-09 16:06:39,804› Facebook - Google Chrome› 'e'
2019-07-09 16:06:39,943› Facebook - Google Chrome› 'y'
2019-07-09 16:06:40,129› Facebook - Google Chrome› 'l'
2019-07-09 16:06:40,277› Facebook - Google Chrome› 'o'
2019-07-09 16:06:40,482› Facebook - Google Chrome› 'g'
2019-07-09 16:06:40,585› Facebook - Google Chrome› 'g'
2019-07-09 16:06:40,703› Facebook - Google Chrome› 'e'
2019-07-09 16:06:40,866› Facebook - Google Chrome› 'r'
2019-07-09 16:06:41,306› Facebook - Google Chrome› '.'
```

ATAQUES INTERNOS

Keyboard loggin – Métodos de infecção

- E-mails de phishing que incluem um anexo que contém a ameaça.
- Download de software em um site duvidoso no qual o keylogger foi incorporado.
- Sites comprometidos (javascsript - XSS) ou em um dispositivo USB, entre outros

ATAQUES INTERNOS

Keyboard loggin – Como se previnir

- Usar e manter sempre atualizado um bom antivírus.
- Usar um gerenciador de senhas seguro, por exemplo o KeePass ou outros, evitando digitar a senha nos sites que deseja acessar.
- Implementando a autenticação em dois fatores.
- Instalar apenas programas de fontes confiáveis.
- Bloquear o dispositivo quando não estiver em uso para evitar que outra pessoa possa instalar um keylogger.

Exemplo de um keylogger que pode ser usado com boa ou má intenção: https://www.refog.com/br/

ATAQUES EXTERNOS

Negação de serviço – DDoS (Distributed Denial of Service)

- É um tipo de ataque que visa sobrecarregar servidores e dessa forma impedir que os usuários legítimos tenham acesso às informações no servidor.
- Podem ser servidores de vários tipos: links de internet, servidores web, servidores de sistemas on-line, servidores de e-mail, etc.
- Quando um servidor fica sobrecarregado, ele gera muita lentidão e não é possível que os usuários se conectem nele. Botnets podem ser usados.
- Exemplo: Um provedor de internet sofre um ataque DDoS; os clientes que usam a internet desse provedor ficam sem internet e não podem mais navegar nos sites, acessar sistemas ou redes sociais.
- Fere o pilar da disponibilidade na Segurança da Informação

ATAQUES EXTERNOS

Negação de serviço – DDoS (Distributed Denial of Service)

Ataque de negação de serviço – DoS/DDoS

Cloudflare diz que conteve o maior ataque DDoS já registrado na história

ATAQUES EXTERNOS

Sniffing ou sniffer de rede – Farejador de rede

- Metodologia que através de aplicativos específicos consegue analisar todo o tráfego de rede, tudo o que "passa" na rede.
- Toda conexão, IP origem, IP de destino, protocolo utilizado é mapeado e "farejado" pelo sniffer.
- Pode ser usado por um administrador da rede para analisar o que se passa na rede e também pode ser usado por ciber criminosos para descobrir conexões que a vítima faz e filtrar informações passadas pela rede.
  https://www.youtube.com/watch?v=24K4HywNcbw

Exemplo de um sniffer

ATAQUES EXTERNOS

Engenharia Social

- Engenharia social é uma técnica usada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites maliciosos.

- Nos crimes virtuais, esses golpes geralmente atingem pessoas desavisadas ou sem muita experiência no mundo virtual. As vítimas podem ter desde seus dados roubados até mesmo seus computadores infectados com vírus. Além disso, os ataques podem acontecer tanto online quanto por telefone ou outros tipos de comunicação.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Existem vários tipos de ataques de engenharia social, sempre tentando usar situações humanas para induzir a pessoa a algum erro. Confira os tipos principais a seguir:

Quid pro quo:

Já recebeu aquele e-mail falando que ganhou uma bolada de dinheiro, e que para receber a quantia, bastava enviar seu CPF ou algum outro dado pessoal para o remetente, não? Esse é a engenharia social chamada de Quid pro quo.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Quid pro quo: expressão em latim que significa “tomar uma coisa por outra”.

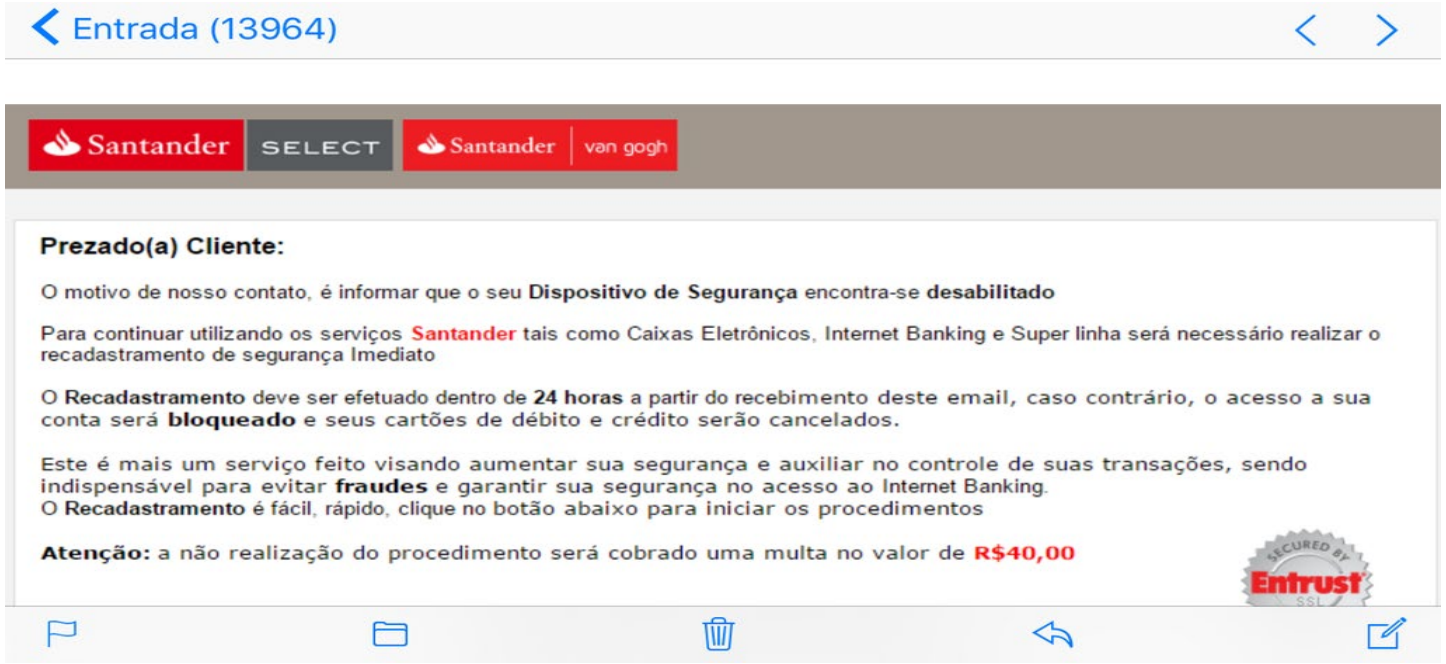
É uma prática muito comum em ataques virtuais, sendo usado desde ransomware até os chamados "scareware", onde uma mensagem promete aos usuários de computador uma atualização para cuidar de um problema de segurança urgente quando, na verdade, o próprio comunicado é a ameaça.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Phishing: já visto anteriormente.



ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Isca: A isca é um método que envolve a criação de uma armadilha, tal como um pen drive USB carregado com malware. Uma vítima encontra o dispositivo e, curioso para ver o que está no aparelho, coloca-o na sua unidade USB, o que resulta num comprometimento do sistema.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Spamming de contatos e hacking de e-mails

E-mails comprometidos em vazamento de dados podem ser sequestrados por invasores que os usam para enviar mensagens com arquivos maliciosos para toda lista de contato da conta, o chamado "spamming de contatos”. Já recebeu aquele “confira esse site incrível” do e-mail do seu irmão? Melhor desconfiar.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Spamming de contatos e hacking de e-mails

Em alguns casos, os criminosos podem invadir uma conta de e-mail sem que os dados de acesso dela estejam vazados, com o intuito de realizar o spamming de contatos.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Pretexto

Alguns criminosos fazem uso de pretextos, ou seja, histórias, para tentar fisgar as vítimas.
Apelando para a inclinação humana de querer ajudar os outros, usuários recebem e-mails de príncipes nigerianos que perderam recentemente seu pai, e que precisam de 500 reais para poderem assumir o trono.
A pessoa, comovida com a narrativa, clica no link do e-mail e acaba baixando vários vírus em seu computador.

ATAQUES EXTERNOS

Engenharia Social

Tipos de engenharia social

Cultivo

Alguns casos de engenharia social podem envolver até mesmo comunicação direta entre o invasor e a possível vítima, com a construção de uma relação entre os dois enquanto na verdade o invasor só quer roubar dados.

Casos até mesmo de pessoas fingindo estar apaixonadas por uma vítima podem ocorrer, onde a vulnerabilidade causada pelo período das emoções à flor da pele acaba fazendo com que a pessoa vaze informações sensíveis para a outra.

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

É difícil se defender da engenharia social, já que essas fraudes são feitas para explorar impulsos e erros humanos, que não são tão simples de arrumar quanto uma atualização de software.

Existem várias dicas que podem ajudar você a melhor identificar e se prevenir de tentativas de golpe. Na maioria das vezes são procedimentos para checar a veracidade das informações recebidas, um processo necessário e importante.

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

Existem várias dicas que podem ajudar você a melhor identificar e se prevenir de tentativas de golpe. Na maioria das vezes são procedimentos para checar a veracidade das informações recebidas, um processo necessário e importante.

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

Confira a fonte

Recebeu um e-mail de uma empresa? Cheque o remetente.

Achou uma unidade USB do nada em sua mesa? Tente traçar a origem do dispositivo antes de o conectar em seu computador.

Checar a fonte é um processo que não demanda muito esforço, e que pode poupar muito estresse no futuro

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

Veja o que eles sabem sobre você

Você recebeu um telefonema do banco e ele não começou com o atendente fazendo perguntas de segurança, mas sim perguntando seu nome ou algum outro dado pessoal? É bem possível que era um golpe.

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

Mantenha a calma

A engenharia social muitas vezes depende de um senso de urgência.

Em um exemplo fora do mundo digital, se você recebe um telefonema falando que sua mãe foi sequestrada, sua primeira reação é ficar desesperado.

Porém, se você se acalma e entra em contato com ela, o bandido perde toda a vantagem que tinha no golpe.

ATAQUES EXTERNOS

Engenharia Social

Como se proteger da engenharia social

Peça identificação

Recebeu um telefonema que de cara já está pedindo várias informações pessoais?

Pergunte com quem o telefonista trabalha e qual o nome dele, ou desligue e vá entrar em contato com os números oficiais da instituição.

Não aceite de cara os questionamentos, trate com cuidado os seus dados e sempre investigue o que realmente está acontecendo.

ATAQUES EXTERNOS

Engenharia Social

Hackers: Guccifer e engenharia social

https://www.youtube.com/watch?v=y9lAbV5l66Q

Garoto de 18 anos usa técnicas de Engenharia Social para invadir TI da UBER

https://www.youtube.com/watch?v=5svS92raMok

DÚVIDAS?