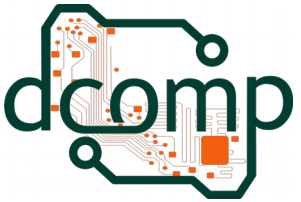
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCENS UFES
Departamento de Computação



Ataques em redes de computadores

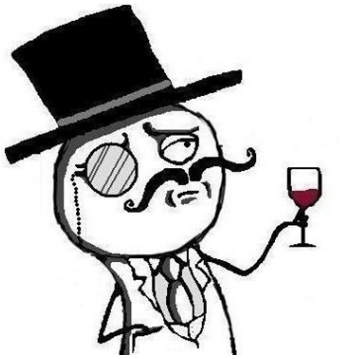
Computação Forense
Site: http://jeiks.net
E-mail: jacsonrcsilva@gmail.com

Inicialmente, se conscientizando...

- É importante ter em mente os passos que correspondem a um ataque.

- Porém, é importante sempre lembrar que
  - alguns invasores são mais inteligentes que a pessoa que implementou a segurança;
  - que vários invasores são imprevisíveis;
  - que a prevenção eventualmente falha.

Quem pode invadir?



- Pessoas com conhecimento técnico.
- Atualmente, qualquer pessoa com acesso à Internet e interesse em aprender, pois possuem:
  - acesso à sites de ajuda;
  - acesso à scripts prontos;
  - acesso à tutoriais de ataque.
- A Internet fornece conteúdo facilitado e atualizado:
  - ensinando a burlar os sistemas de segurança;
  - permitindo que pessoas com pouco conhecimento ataquem computadores com ou sem proteção.

O que leva à invasão?

- Ato de descobrir vulnerabilidades no sistema, para
  - simplesmente para divulgar a falha,
  - ou para utilizar o sistema,
  - para ganhar status, etc.
- Ato de danificar um sistema,
  - por diversão,
  - por concorrência, etc.
- Ato de obter os dados importantes do sistema
  - para utilização própria,
  - para terceiros, etc.
- Ou simplesmente por prazer...

Outros fatores que levam à invasão

- Espionagem industrial;
- Proveito próprio;
- Inexperiência;
- Vingança;
- Status ou Necessidade de Aceitação;
- Curiosidade e Aprendizado;
- Busca de aventuras;
- Maldade;
- Acabar com a corrupção;
- Diversos outros motivos...

Uma curiosidade...

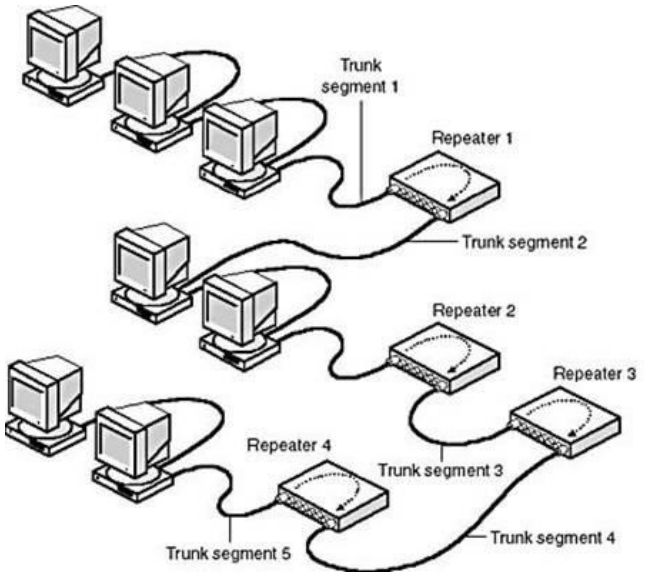
- Na *Filosofia Hacker*, um atacante:
  - deve estudar e obter o maior conhecimento possível,
  - não pode ficar se exibindo, se achando o tal,
  - não deve cometer atitudes *Lammer*,
  - deve deixar um sistema com sua falha para uma possível utilização futura.

Tipos de atacantes

- Curiosos:
  - Geralmente estudantes procurando diversão.
- In-house:
  - Funcionários ou ex-funcionários de empresas.
- Técnicos:
  - Gostam de criar programas e compartilhar com os outros, possuem muito conhecimento.
- Profissionais:
  - Aqueles que recebem pelo que fazem.

O atacante...

- Os passos de um atacante envolvem:
  - Reconhecimento da rede;
  - Exploração da rede;
  - O reforço;
  - A consolidação dos planos;
  - E o saque.



- Com esses passos o invasor pode tirar vantagem de uma vítima.

Reconhecimento

- Processo de:
  - validar a conectividade,
  - enumerar os serviços e
  - verificar por vulnerabilidade de aplicações
- Como obter informações de um servidor:
  - Fornecendo pacotes válidos TCP ou UDP;
  - Para comunicar com o servidor, pois precisa utilizar sua linguagem e suas regras.
- Pode-se também fazer uma busca detalhada de informações sobre o alvo.

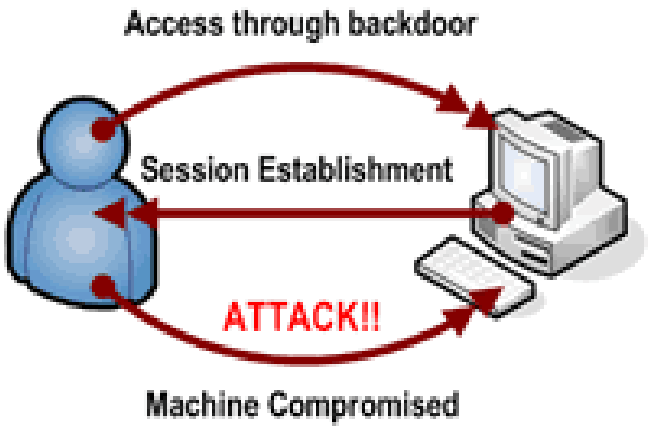
Exploração

- Processo de violação, que corrompe ou penetra os serviços de um alvo.
- Alguns exemplos de violação são:
  - acessar o servidor por algum serviço utilizando um acesso legítimo ou não;
  - criar uma execução de um serviço não prevista por seus programadores;
  - acessar um sistema, ganhando privilégios sem interromper o serviço fornecido.

Reforço

- Processo onde o intruso aproveita o acesso sem autorização,
  - Verifica falhas e ganha mais capacidades no alvo.
- Geralmente, instalam meios de comunicar com o mundo externo. Ex:
  - *backdoors:* túneis de acesso mais complicados de serem encontrados:
    - *servidor.py* e *cliente.py*
    - *Servidor: nc -l -p porta -e /bin/bash*

      Cliente: nc IP porta



Consolidação

- Processo de comunicação do intruso ao alvo com um *backdoor*.
- Há três casos de sua consolidação:
  - Abrir uma porta por onde um invasor pode se conectar ao programa do *backdoor*;
  - Fazer o programa do *backdoor* se conectar ao IP do invasor;
  - Fazer o programa do *backdoor* se conectar a um Internet Relay Chat (IRC) para receber as instruções de funcionamento.

Saque

- Envolve:
  - roubar informações do alvo,
  - construir uma base de ataques, ou
  - fazer qualquer outra coisa que o invasor deseje.

A detecção do invasor

- No reconhecimento:
  - *a probabilidade de detecção é de média para alta.*
  - os atacantes devem executar serviços de descoberta durante um longo tempo, utilizando padrões normais de tráfego.
    - Só assim podem catalogar as máquinas, os serviços e as aplicações.
  - Nesse momento, os atacantes revelam-se pelas diferenças entre seu tráfego e o tráfego legítimo de um usuário.
  - Ex: nmap

A Detecção do Invasor

- Na exploração:
  - *a probabilidade de detecção é alta.*
  - para efetuar tentativas de acesso, os atacantes utilizam *exploits* nos serviços oferecidos.
  - Essas ferramentas não apresentam um tráfego legítimo.
  - Pode ser detectado por Sistemas de Detecção de Intrusos.

A Detecção do Invasor

- No reforço:
  - *a probabilidade de detecção é alta.*
  - as ferramentas utilizadas pelos atacantes para obter mais privilégios ou para disfarçar a invasão causam uma atividade suspeita nos servidores.
  - essa atividade pode ser facilmente acompanhada e identificada.

A Detecção do Invasor

- Na consolidação
  - *a probabilidade de detecção é de baixa para média*
  - o atacante tem o controle total através da comunicação de sua máquina com a máquina alvo
  - seus limites são impostos somente pelo controle de acesso e de tráfego dos dispositivos da rede
  - O perfil do tráfego é o único que pode identificar padrões desconhecidos que correspondem a utilização do *backdoor* pelo atacante

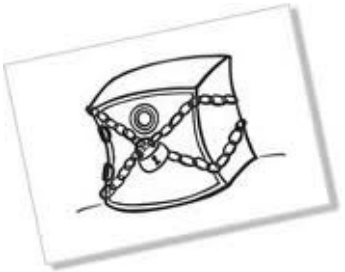
A Detecção do Invasor

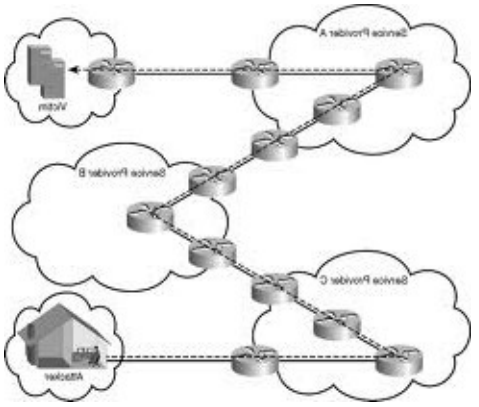
- No saque
  - *a probabilidade de detecção é de baixa para média*
  - o tráfego do atacante vem de uma máquina “de confiança”
  - Uma forma possível para detecção
    - conhecer o trabalho dos sistemas internos
    - detectar divergências

O Processo de Segurança

Processo de Segurança

- Segurança é um processo e não um estado.
- Envolve quatro passos
  - de avaliação,
  - de proteção,
  - de detecção e
  - de resposta ao ocorrido.





Avaliação

- Envolve determinar medidas que possam garantir a probabilidade de sucesso ao defender uma empresa ou instituição.
- Deve-se definir
  - Uma política de segurança
  - Os serviços que estarão disponíveis em uma empresa
- Este passo define como será o tráfego da instituição
- Se a política definida for realmente rigorosa, qualquer outro tráfego não conhecido é um incidente na rede, sendo ou não um ataque
- Os incidentes originam também de tentativas de usuários internos de escaparem das regras
- A equipe de gerência define como invasão ou somente violação da política
  - Porém, sempre se baseiam na política de segurança adotada

Proteção

- É a aplicação das medidas defensivas
- Visa reduzir a probabilidade de incidentes
- Problema crítico na auditoria de tráfego
  - Quantidade de tráfego que deve ser monitorada
    - Deve-se reduzir a quantidade de tráfego ou as formas de acesso
    - Assim, tem-se um tráfego menor para monitorar e analisar

Detecção

- É o processo de identificar os intrusos
  - coletando,
  - identificando,
  - validando e
  - escalonando eventos suspeitos
- As invasões são
  - violações da política ou
  - acidentes na segurança dos computadores de uma rede

Detecção

- Requer quatro passos:
  - Coletar: inspecionar e armazenar informações úteis do tráfego da rede
  - Identificar: obter informações do tráfego e então, classificá-lo em: Normal; Suspeito; Malicioso
  - Validar: atribuir aos eventos uma categoria de incidente preliminar.
    - Definição se necessita de mais investigação
  - Escalonar: encaminhar os eventos obtidos às pessoas que tomarão decisões

Detecção - Validação

- Os eventos podem ser assimilados em uma das categorias:
  - acesso sem autorização como administrador
  - acesso de usuário sem autorização
  - tentativas de acesso sem autorização
  - ataque de negação de serviço com sucesso
  - prática de segurança ruim ou violação da política
  - reconhecimento/provas/explorações
  - infecção por vírus

Resposta

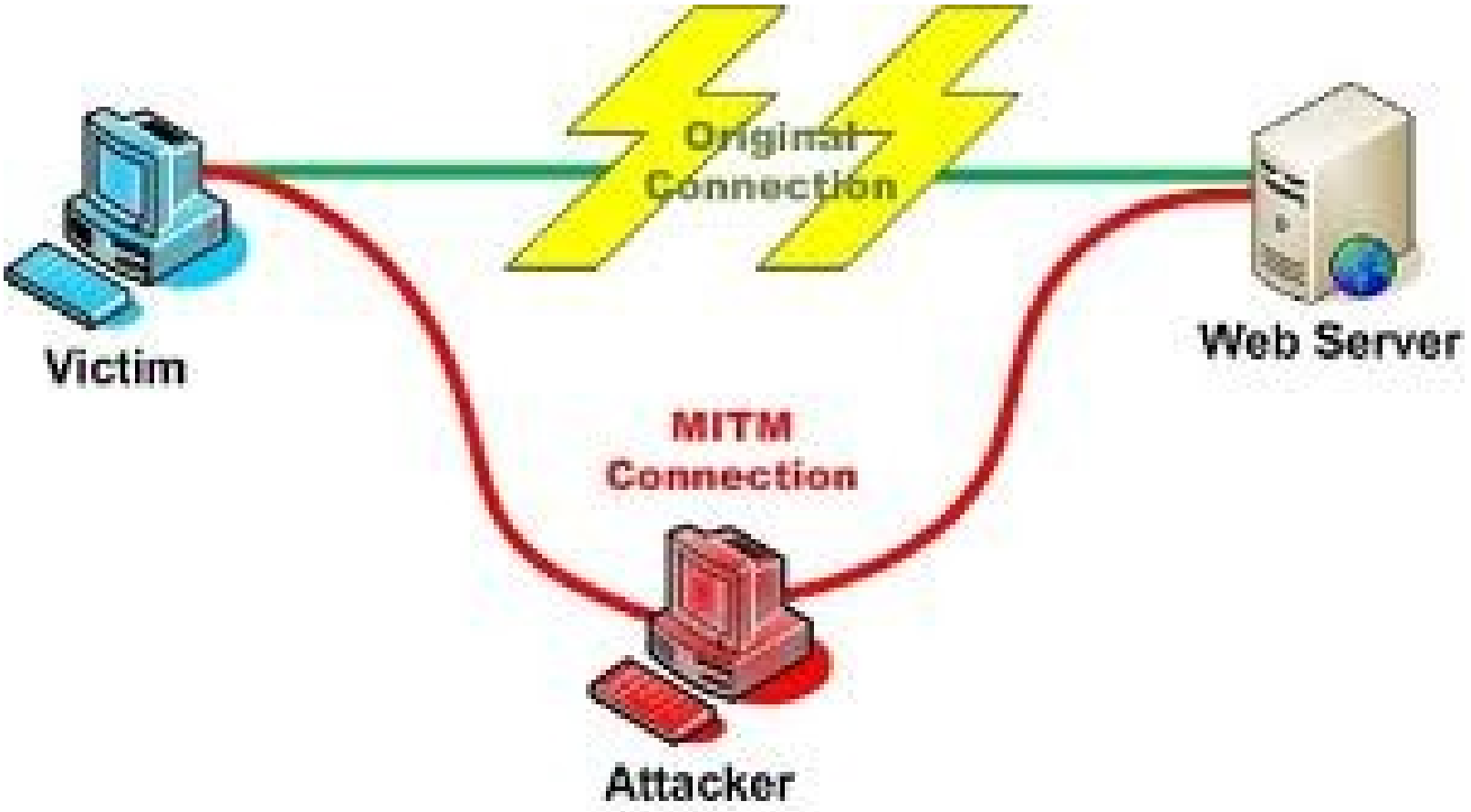
- É o processo de
  - validar os frutos da detecção e
  - tomar medidas para remediar as invasões
- Existem dois processos de resposta
  - contenção do incidente em curto prazo
    - consiste em impedir que o incidente continue na rede
    - Ex: impedir fisicamente o acesso à máquina alvo
      ou instalar uma nova regra no *firewall* para proibir o tráfego
  - monitoramento de emergência
    - consiste em capturar todos os dados sobre o IP invasor
    - quando todo o tráfego já é armazenado, isso não é necessário

Tipos de Ataques

Furto e quebra de senhas

- O arquivo de senha roubado de um servidor é submetido a quebra por uma ferramenta de crack de senha.
- Assim é obtido as senhas dos usuários que tiveram seu servidor invadido.
- John The Ripper

Homem do Meio



Negação de Serviço (DoS)

- Sobrecarga de um servidor com uma quantidade excessiva de solicitações de serviços
- Existem ataques DoS distribuídos (DDoS)
  - o invasor invade muitos computadores
  - e instala neles um software zumbi;
  - Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor alvo

Engenharia Social

- *...Sexta feira as 16:00 da tarde o operador do CPD de uma grande empresa recebe um telefonema do "diretor financeiro" solicitando sua senha para trabalhar remotamente, o operador gentilmente fornece a informação e no outro dia vai descobrir que foi enganado.*
- Este é um exemplo do expediente usado para este tipo de ataque.

Falhas de Autenticação

- Um programa pede para efetuar o login

  Username: marcia

  Password: ********
- Explorando falhas,
  - o programa de login pode ser atacado
  - e pode fornecer acesso sem nome e/ou senha

- *Exemplo com shell...*

Falhas de Protocolos

- Ataques DoS (negação de serviço)
  - Reinicia ou para o serviço
  - Ou causa lentidão
- Ataque LAND
  - Um invasor emite pacotes de requisição de conexão com endereços IPs de origem e destino

Spoofing

- Usar uma máquina para fazer de conta que é outra
- Pode-se
  - forjar o endereço de origem de um ou mais *hosts*
  - atacar o DNS
  - atacar como máquina do meio
- Para realizar uma sessão bem sucedida de *spoofing*, costuma-se “matar” temporariamente a máquina que está personificando
- *Exemplos....*

Vazamento de informação

- Obtido através da resposta a consulta de
  - Ping,
  - Traceroute,
  - Telnet,
  - Nmap,
  - etc.
- Informações de versões de SO e *hosts*
  - Fornecem ao invasor informações que o permitirá planejar seu ataque a rede
  - Ex: NmapSI4

Mail Bomb

- Milhares de mensagens enviadas a uma caixa postal
- O objetivo do atacante é
  - apenas enviar lixo para a caixa postal de alguém
  - e congestionar a via de acesso corporativo à Internet
- Existem diversos programas que automatizam o *mail bombing*

Cavalos de Troia

- O termo vem de uma passagem da Ilíada de Homero, na qual os gregos deram de presente um imenso cavalo de madeira a seus inimigos, os troianos, aparentemente como oferta de uma proposta de paz.
- Por analogia, hoje na informática, o termo *trojan* ou *cavalo de troia* é usado para designar uma categoria de programas destrutivos mascarados em programas e aplicativos

Sondagem (*Probing*)

- Escanear a rede com *scanners*
  - programas que buscam portas TCP abertas por onde pode ser feita uma invasão
- Para evitar a detecção,
  - alguns *scanners* testam portas de um computador durante muitos dias em horários aleatórios

Smurf

- Um tipo de ataque de negação de serviço
- Como funciona
  - O agressor envia solicitações de ping para um endereço de *broadcast*
  - Usando *spoofing*, o cracker faz com que o servidor de *broadcast* encaminhe as respostas não para seu endereço, mas para o da vítima
  - Assim, o computador-alvo é inundado pelo ping

Sniffing

- Programa ou dispositivo que captura o tráfego de rede
- São úteis para gerenciamento de redes
- Mas nas mãos crackers permitem roubar senhas e outras informações sigilosas

- *Exemplo...*

Ping da Morte

- É o envio de um pacote IP com tamanho maior que o máximo permitido (65535 bytes) para a máquina que se deseja atacar
- O pacote é enviado na forma de fragmentos e quando a máquina destino tenta montar estes fragmentos, inúmeras situações podem ocorrer:
  - a maioria da máquinas trava,
  - algumas reinicializam,
  - outras abortam e mostram mensagens no console...

Ataque de *replay*

- Forma particular de ataque em que parte de uma transmissão de rede é gravada e reproduzida posteriormente.
- Normalmente, esse tipo de ataque está associado a uma criptografia mal estruturada
- Onde está o problema
  - credencial for codificada sempre da mesma maneira;
  - o atacante pode gravar a sequência criptografada
  - e incorporá-la em uma transmissão realizada por ele mesmo
  - Assim, sem saber a senha, seria possível conseguir acesso ao sistema.