Parte II

- Tipos de Ataques

Tipos de Ataques

- Negação de Serviço
- Vazamento de Informações
- Acesso a arquivos comuns
- Informação Falsa
- Acesso a arquivos ou bancos de dados especiais
- Execução remota de código arbitrário
- Elevação de Privilégios

Negação de Serviço (Denial of Service)

- Quando a disponibilidade de um recurso é intencionalmente bloqueada ou prejudicada.

- O ataque impede a disponibilidade do recurso para seus usuários autorizados regulares.

Negação de Serviço

- Dificultar processos.
- Diminuir a capacidade de armazenamento.
- Destruir arquivos para tornar o recurso inutilizável.
- Desativar partes do sistema ou processos.

Negação de Serviço

- O ataque é local. São comuns.
- Muitos casos inevitáveis.
- São mais fáceis de detectar.
- Desde que a infra-estrutura de segurança esteja correta, são facilmente rastreados e o atacante é facilmente identificado.

Negação de Serviço

- Degradação de processo.
- Esgotamento de espaço em disco.
- Esgotamento de nó de índice.

Degradação de processo

- No kernel Linux até a versão 2.4.12 ... ... O *scheduler* de processos podia ser bloqueado, impedindo que quaisquer outros processos no sistema recebessem tempo de CPU.

Degradação de processo

- Ataque local.
- Afetando outros sistemas operacionais, existe o *fork bomb*.
- Diminui o desempenho de processos com efeitos variáveis.
- O efeito pode ser tão pequeno quanto fazer o sistema operacional funcionar lentamente ...

Degradação de processo

- Ou podem ser tão extremos quanto monopolizar recursos do sistema operacional, causando sua queda.
- O código para shell: $ 0 & $ 0 &
- O código para C:

  (main() {for(; ;) fork () ; })

Esgotamento do espaço em disco

- Ataque local.
- O espaço em disco é um recurso finito.
- Consumir o espaço em disco até sua capacidade máxima.
- O espaço em disco era um recurso extremamente caro.
- A indústria atual tem diminuído o preço do armazenamento em disco.

Esgotamento do espaço em disco

- Pode-se resolver muitos problemas de armazenamento com soluções como *arrays* de disco e software que monitora o excesso de armazenamento.

Esgotamento do espaço em disco

- O espaço em disco continua sendo um entrave para todos os sistemas. As soluções baseadas em software, com cotas de armazenamento por usuário, visam amenizar este problema.

Esgotamento do espaço em disco

- O ataque impede a criação de novos arquivos e o crescimento dos arquivos existentes.

- Alguns sistemas UNIX cairão quando a partição raiz atingir a capacidade de armazenamento.

Esgotamento do espaço em disco

- Incluir uma partição separada para os recursos de *log,* como o /var, e uma partição separada para os usuários como o diretório /home no LINUX ou /export/home nos sistemas SUN.

Esgotamento do espaço em disco

- Objetivo do ataque: derrubar sistemas, quando o *layout* de disco não for feito com partições de *log* e de usuários em separado.

Esgotamento do espaço em disco

- Outro objetivo: obscurecer as atividades de um usuário, gerando grande quantidade de eventos que são registrados via *syslog*, enchendo a partição onde os *logs* são armazenados e impossibilitando o *syslog* de qualquer outra atividade.

Esgotamento do espaço em disco

- Outro objetivo: obscurecer as atividades de um usuário, gerando grande quantidade de eventos que são registrados via *syslog*, enchendo a partição onde os *logs* são armazenados e impossibilitando o *syslog* de qualquer outra atividade.

Esgotamento do espaço em disco

- O ataque: um usuário local executa o comando

  cat /dev/zero > ~maliciousfile

- O comando concatena dados do arquivo de dispositivo /dev/zero (que simplesmente gera zeros) com o arquivo malicioso, continuando até que o usuário suspenda o processo ou que a partição seja atingida.

Esgotamento de inode

- O ataque é local.
- Concentra-se no sistema de arquivos.
- inode = index node (nó de índice).
- Os nós de índice são parte essencial do sistema de arquivos do UNIX.

Esgotamento de inode

- Contém informações vitais ao gerenciamento do sistema de arquivos: proprietário do arquivo, associação de grupo do arquivo, tipo de arquivo, as permissões, o tamanho e os endereços de bloco contendo os dados do arquivo.

Esgotamento de inode

- Quando um sistema de arquivos é formatado, um número finito de inodes é criado para manipular a indexação dos arquivos.
- O ataque visa usar todos os inodes disponíveis para uma partição.

Esgotamento de inode

- O sistema é incapaz de criar novos arquivos.
- Objetivos do ataque: impedir o registro dos eventos de sistema, especialmente, as atividades do próprio *hacker*.

INODE

- Em UNIX, pode-se verificar quantos inodes estão livres sobre um disco por emitir o comando *df* com a opção –i:

- % df -o i /usr

Negação de Serviço (Ataque Remoto)

- Ataques de negação de serviço lançados através de uma rede.

- Duas categorias:

  - um ataque que afeta um serviço específico;

  - um ataque que visa um sistema inteiro.

Negação de Serviço (Ataque Remoto)

- Ferramentas disponíveis conferem anonimato e capacidade de causar um problema exigindo pouco conhecimento técnico.

Negação de Serviço (Ataque Remoto)

- A gravidade desses ataques varia significativamente.
- São destinados a produzir transtornos.
- Lançados como uma ação retaliatória.

Negação de Serviço (Ataque Remoto)

- Lado do Cliente
- Baseado em Serviço
- Direcionada a Sistema

Negação de Serviço (Ataque Remoto)

- DoS direcionada a sistema
  - Ataques de Flooding

Flooding

- Usado para prejudicar o desempenho ou tornar o sistema completamente indisponível.

- Forma de ataque: usar uma exploração para atacar um sistema por meio de outro, deixando o sistema alvo inoperante.

Flooding

- O conceito de inundação (flooding) de SYN (.
- Ataque lançado de qualquer sistema em uma rede mais rápida que o sistema-alvo, para múltiplos sistemas.

Flooding

- É usado para degradar desempenho de sistema.
- A inundação de SYN (sincronização) é realizada enviando requisições de conexão IP mais rápido do que um sistema pode processar.

Flooding

- Como o sistema-alvo consome recursos para cuidar de cada conexão, um grande número de SYNs chegando, pode levar o sistema-alvo a ficar sem recursos para novas conexões legítimas.

Flooding

- O endereço IP de origem é falsificado, para quando o sistema-alvo tentar responder com um SYN-ACK (sincronização-confirmação), o atacante não recebe resposta alguma.

Flooding

- O código de exploração para o flooder de SYN, syn4k.c foi escrito por Zakath.

- Este flooder de SYN permite selecionar as portas e um endereço, a inundar no sistema-alvo.

Flooding

- O código pode ser obtido em:

  www.cotse.com/sw/dos/syn/synk4.c
- Pode-se detectar uma inundação de SYN feito pelo código synk4.c usando-se o comando netstat (Windows).
- C:WINNT\System32\cmd.exe
- C:\>netstat -n -p tcp
- C:\>netstat -all

Flooding

- C:WINNT\System32\cmd.exe
- C:\>netstat -n -p tcp
- -n exibe o <endereço IP:porta> (Local Address) atingido e o endereço remoto (Foreign Address) de onde vem a inundação.
- -p seleciona o protocolo desejado.
- C:\>netstat -n -p udp
- São mostradas as conexões que interessam para o ataque em particular.

Negação de Serviço (Ataque Remoto)

- DoS de rede direcionada a sistema
  - Ataques Smurfing

Smurfing

- Geralmente lançados pelos *scripts kiddiots* (script do atacante), com poder de anonimato.
- O ataque de *smurf* realiza um DoS através de rede contra um host-alvo.
- O ataque se baseia na ajuda de um intermediário, um roteador.

Smurfing

- O atacante falsificando o endereço IP de origem, gera uma grande quantidade de tráfego de *echo* ICMP (Internet Control Message Protocol) direcionado aos endereços de *broadcast* IP, no roteador.

Smurfing

- O roteador, chamado de *amplificador de smurf*, converte o *broadcast* IP em um *broadcast* da camada 2 (enlace) e a passa adiante.

Smurfing

- Cada *host* que recebe o *broadcast*, responde para o endereço IP falsificado, com uma resposta de *echo*.

Smurfing

- Dependendo do número de hosts na rede, tanto o roteador, tanto o host-alvo podem ser inundados com tráfego.

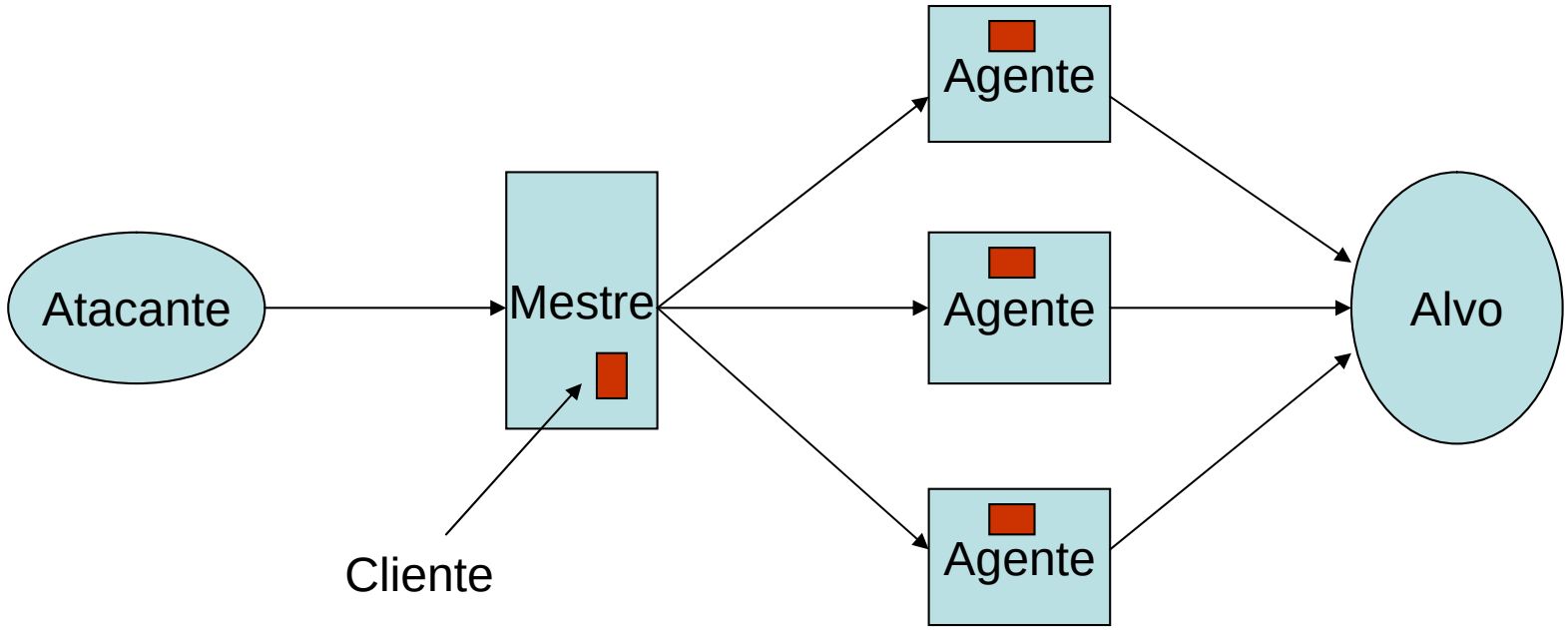
Smurfing

- Isto pode resultar na queda de desempenho na rede, do host-alvo sendo atacado e, dependendo do número de redes com roteadores amplificadores usados, a rede com o host-alvo, se torna saturada até a sua capacidade.

Negação de Serviço (Ataque Remoto)

- DoS direcionada a sistema
  - Ataques DDoS

DDoS



DDoS

- Atacante – Quem efetivamente coordena o ataque.
- Master – Máquina que recebe os parâmetros para o ataque e comanda os agentes.
- Agente – Máquina que efetivamente concretiza o ataque DoS contra um ou mais alvos, conforme especificado pelo atacante.

DDoS

- Alvo do ataque – Máquina que é “inundada” por um volume grande de pacotes, ocasionando um congestionamento extremo da rede e resultando na paralização dos serviços oferecidos pela mesma.

DDoS

- Cliente – Aplicação que reside no *Master* e que efetivamente controla os ataques enviando comandos aos *daemons*.

- *Daemons* – Processos que roda nos agentes, responsável por receber e executar os comandos enviados pelo cliente.

DDoS

- Resulta de conjugar os dois conceitos:
  - negação de serviço
  - intrusão distribuída.

- Ataques DoS partindo de várias origens, disparados simultaneamente e coordenadamente sobre um ou mais alvos.

DDoS

- O ataque é dado em três fases:

  - Uma fase de intrusão, na qual ferramentas automáticas são usadas para comprometer máquinas e obter acesso privilegiado (acesso de root).

DDoS

- o atacante instala software DDoS (agentes) na máquinas invadidas, para montar a rede de ataque.

- fase da inundação, consolidando o ataque.

DDoS

- Fase 1: Intrusão em Massa

- É realizada uma varredura de portas e vulnerabilidades em redes consideradas “interessantes”.
- Explorar as vulnerabilidades reportadas para a obtenção de acesso privilegiado nessas máquinas.

DDoS

- *Sniffers* e *Rootkits*
- Um *Sniffer* é um programa ou ferramenta que monitora uma rede em busca de informações em que o atacante possa estar interessado.
- Informações de autenticação, como nomes de usuários e senhas.

DDoS

- *Sniffers* são incluídos na maior parte dos *Rootkits*.

- É criada uma lista de IPs das máquinas que foram invadidas e que serão utilizadas na montagem da rede.

DDoS

- Fase 2: Instalação de Software DDoS

- Uma conta de usuário qualquer é usada como repositório das versões compiladas de todas as ferramentas de ataque DDoS.

DDoS

- Uma vez que a máquina seja invadida, os binários das ferramentas DDoS são instalados nessas máquinas para permitir que sejam controladas remotamente.

- Masters ou Agentes.

DDoS

- Masters, não devem ser máquinas manuseadas cosntantemente pelos administradores.

- Agentes devem estar em máquinas conectadas à Internet por *links* relativamente rápidos.

DDoS

- Rodados os *daemons* que rodam nos agentes, esses se anunciam para os *masters* e ficam à espera de comandos.

- A aplicação DDoS que roda nos *masters*, registra em uma lista IP das máquinas agentes ativas.

DDoS

- Essa lista pode ser acessada pela máquina atacante.
- A partir da comunicação automatizada entre *masters* e agentes, organizam-se os ataques.
- Rootkits poderão ser instalados para ocultar o comprometimento das máquinas.

DDoS

- Fase 3: O ataque

- O atacante controla um ou mais máquinas *masters*, as quais por sua vez podem controlar um grande número de máquinas agentes.
- A partir dos agentes é disparado o “flood” de pacotes que consolida o ataque.

DDoS

- Quando o atacante ordena o ataque, uma ou mais máquinas-alvo são inundadas por um volume considerável de pacotes, resultando na saturação do link de rede e paralização dos seus serviços.

Ferramentas de DDoS

- Fapi
- Blitznet
- Trin00 (**)
- TFN (**)
- Stacheldraht (**)
- Shaft
- TFN2K (**)
- Trank
- Trin00 win version