Fatec São Caetano do Sul

Segurança em Sistemas Operacionais e Redes de Computadores II

Ataque de DDOS e Brute Force

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DDoS – Brute Force

- DDoS – Distributed Denial of Service (Negação de serviço distribuído)
- Brute Force (de autenticação)
- De maneira geral, uma vez descobertas as vulnerabilidades na fase 2 os atacantes passam para a fase 3 com 2 objetivos:
  - Ganhar acesso ao sistema usando técnicas como “brute force”, IP spoofing, sniffing, etc...;
  - Negar o acesso a usuários legítimos ou interromper serviços críticos usando técnicas como DDoS.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

Brute Force – Senhas/SIDs

Ataques que consistem em verificar sistematicamente prováveis candidatos a senhas através de “dicionários” (palavras e frases) ou mesmo todas as combinações possíveis

- Banco de dados
  - MS-SQL server: mssql_login, Fast-track,
  - ORACLE: sid_brute (SID), oracle_login (senhas) e OAT (Oracle Auditing Tools) (senhas)
- SNMP
  - Onesixtyone, hydra.
- Telnet, HTTP, HTTPS, Cisco, VNC
  - Hydra.
- CGI (Common Gateway Interface)
  - Whisker

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS – Denial-of-Service

- Categorias de ataques de DoS (Denial-of-Service)
  - Interrupção de serviços;
  - Exaustão de recursos.
- Ambas podem ser locais ou remotas.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS – Categorias

- Ataques de interrupção de serviços:
  - Locais: Encerramento de processos (process killing), “quebra” de processos (process crashing), reconfigurar o sistema;
  - Remotos: Ataque de pacotes defeituosos (malformed packets). Ex: Land, bonk Rose, etc...
- Ataques de exaustão de recursos
  - Locais: Criar processos em grande quantidade para lotar a tabela de processos, preencher todo o sistema de arquivos;
  - Remotos: Inundação de pacotes (packet flood). Ex: smurf, SYN Flood, DDoS, etc.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques locais de interrupção de serviços:
  - Encerramento de processos (process killing) – Efetuado em um DoS quando o atacante tem privilégios suficientes (UNIX: root, Windows: administrador);
  - Reconfiguração de serviços: Efetuado em um DoS quando o atacante tem privilégios suficientes negando acesso a usuários legítimos e/ou fazendo com que serviços não sejam mais iniciados (como um servidor web por exemplo);
  - “Quebra” de processos (process crashing) - Efetuado em um DoS mesmo sem ter privilégios suficientes explorando vulnerabilidades do sistema.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Defesas para os ataques locais de interrupção de serviços
  - Manter o sistema atualizado;
  - Só dar privilégios a quem efetivamente precisa;
  - Rodar programas de verificação de integridade de arquivos tais como o tripwire (www.tripwire.com) ou o AIDE (aide.sourceforge.net).

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques locais de exaustão de recursos:
  - Lotar a tabela de processos: É efetuado, por exemplo, através de um programa que inicia um derivado (fork) de outro processo para que rode uma cópia de si mesmo que por sua vez fará o mesmo e assim por diante;
  - Preencher todo o sistema de arquivos: É efetuado através da gravação contínua de grandes quantidades da dados até que não sobre nenhum espaço livre impedindo que outros gravem no sistema e/ou levando o sistema a “quebrar”;
  - Enviando tráfego de rede para ocupar toda a largura de banda do enlace de comunicação e/ou a capacidade do processador.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Defesas para os ataques locais de exaustão de recursos:
  - Usar o princípio do menor privilégio ao criar e manter contas de usuários, restringir, se possível, os limites de consumo de recursos do sistema por usuário e outros recursos tais como ferramentas de monitoramento como ferramentas de IDS, por exemplo.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques remotos de encerramento de serviços:
  - Muito mais frequentes que os ataques locais de encerramento de serviços;
  - Um dos métodos mais comuns é o ataque de pacotes defeituosos que são enviados para explorar um erro na pilha TCP/IP ou em em serviços que estão sendo executados. Se o sistema é vulnerável ele “quebrará” (crash) encerrando possivelmente um processo específico, a comunicação de rede ou até o encerramento do sistema operacional (system halt)

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques remotos de encerramento de serviços(cont.):
  - Land: Ataca um grande número de plataformas (entre elas Windows e vários clones do UNIX, roteadores, impressoras, etc...). IPs e portas são configuradas com o mesmo valor. Parece que está saindo da porta onde está chegando, confundindo e “quebrando” alguns sistemas com pilhas TCP/IPs mais antigos;
  - Latierra: Também ataca um grande número de plataformas (entre elas Windows e vários clones do UNIX, roteadores, impressoras, etc...). Relativo do Land envia múltiplos pacotes do tipo Land a múltiplas portas simultaneamente.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques remotos de encerramento de serviços (cont.):
  - Ping da Morte (Ping of Death): Ataca um grande número de plataformas (entre elas Windows e vários clones do UNIX, roteadores, impressoras, etc...). Envia pacotes desproporcionalmente grandes. Sistemas TCP/IP mais antigos não conseguem lidar com pacotes de ping fragmentados maiores de 64kilobytes e “quebram” quando tentam remontar essa grande requisição de eco ICMP.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques remotos de encerramento de serviços(cont.):
  - Jolt2: Ataca sistemas Windows. Envia um fluxo de fragmentos de pacotes sendo que nenhum deles tem offset igual a zero (nenhum é o primeiro). Enquanto estiverem sendo enviados, o processo de remontagem consome toda a capacidade de processamento da máquina alvo;
  - Outros: Rose, Teardrop, Newtear, Bonk, Syndrop e Winnuke.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Defesas contra ataques remotos de encerramento de serviços:
  - Manter o sistema atualizado;
  - Criar filtros antispoofing nos roteadores e firewalls de fronteira (derrubar todos os pacotes que vem a uma interface que tem o endereço de origem em uma rede que está em outra interface);
  - Outras técnicas de antispoofing disponíveis.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques remotos de exaustão de recursos
  - São o ataques de DoS mais frequentes;
  - Inundação de SYN (SYN flood): São enviadas grandes quantidades de pacotes SYN com endereços de origem que não respondem (se o endereço de origem tem uma máquina o RESET de resposta termina a conexão liberando os recursos usados na conexão mitigando a eficácia do ataque).

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Defesas para os ataques de SYN Flood
  - Providenciar capacidade adequada de banda e caminhos redundantes para todos os sistemas críticos (considerar dois ou mais provedores de conexões com a Internet);
  - Consultar e implementar recomendações correspondentes ao sistema operacional em uso.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DoS

- Ataques Smurf
  - Envia um ping de broadcast com endereço de origem da vítima fazendo com que receba resposta de todas as máquinas da rede.
- Defesas para os ataques Smurf
  - Providenciar capacidade adequada de banda e caminhos redundantes para todos os sistemas críticos (considerar dois ou mais provedores de conexões com a Internet);
  - Consultar e implementar recomendações correspondentes ao sistema operacional em uso.

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DDoS

- Distributed Denial-of-Service
  - Controla um grande número (pode chegar a centenas de milhares) de máquinas (zumbis). Essas máquinas podem ser servidores de pequenas ou grandes empresas ou de usuários domésticos conectados à Internet através de conexões de banda larga;
  - O software instalado nos zumbis aguarda um comando do atacante que usa uma ferramenta cliente para interagir com os zumbis.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DDoS

- Distributed Denial-of-Service (cont.)
  - De maneira geral o software cliente que controla essas máquinas é um cliente de IRC (Internet Relay Chat) que injeta comandos em um canal compartilhado usado por todos os zumbis;
  - Pode-se utilizar também um software especializado para se comunicar com os zumbis tal como o Tribe Flood Network 2000 (TFN2K).

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DDoS

- Ataques com o TFN2K
  - Inundações de UDPs;
  - Inundações de SYNs;
  - Inundações de ICMPs;
  - Smurfs;
  - “Mix” de ataques que podem incluir inundações de UDPs, SYNs e ICMPs.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

DDoS

- Defesas contra ataques de DDoS
  - Duas estratégias:
    - Manter os zumbis fora do sistema: Manter o sistema atualizado e seguir as boas práticas em relação a anexos de e-mails;
    - Defender-se dos próprios ataques: filtros antispoofing já que os ataques de DDoS quase sempre envolvem pacotes “spoofed”.

Fatec São Caetano do Sul

Ataque de exploração de vulnerabilidades e Ataques DDoS e Brute Force

- Referências

  - FAIRCLOTH, J. **Penetration Tester's Open Source Toolkit** 3rd ed - J. Faircloth, Syngress, 2011.
  - SKODIS E, LISTON T. **Counter Hack Reloaded**, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Prentice Hall, 2005