Segurança Informática

Aula 8

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de proteção e técnicas de defesa
8. Entidades de Segurança

7. Mecanismos de Proteção e Técnicas de Defesa

Objetivos:

* Reconhecer falhas e indicar técnicas de ataque à segurança informática.

* Apontar mecanismos e técnicas de proteção de redes e sistemas.

A Vertente da Engenharia Social

- O termo "engenharia social" (do inglês "social engineering"), representa a arte de influenciar pessoas a fim de controlar mecanismos de segurança.

- Esta técnica compreende em obter informações, por parte dos utilizadores por correio electrónico, por telefone, ou por contacto direto.

- A engenharia social tem como base a utilização da força de persuasão e na exploração da inocência dos utilizadores, fazendo-se o atacante frequentemente passar por uma pessoa que não é, ou consistindo o ataque de um programa com comportamento falso.

A Vertente da Engenharia Social

- Quanto ao porquê de as organizações serem atacadas através de engenharia social, é muitas vezes uma maneira mais fácil de obter acesso ilícito do que a maioria das formas de pirataria técnica.

- Ataques de engenharia social têm lugar em dois níveis:
  - Físico - O ambiente físico para esses ataques: o local de trabalho, o telefone, o lixo, e até mesmo on-line.

  - Psicológico - Um dos meios mais utilizado pelos hackers para obterem esse tipo de senha é através de um formulário on-line: podem enviar algum tipo de informação sobre sorteios e pedir que o utilizador coloque um nome (incluindo e-mail). Outra maneira dos hackers poderem obter informações on-line é, fingirem ser o administrador da rede, enviando e-mails através da rede e pedindo a senha do utilizador.

A Vertente da Engenharia Social

- A personificação geralmente significa a criação de algum tipo de personagem e interpretação de um papel.
- Quanto mais simples o papel a interpretar, melhor, pois o hacker com um papel simples consegue ser mais credível.
- Alguns perfis que podem ser utilizados em ataques de representação incluem: técnico de suporte de TI, administrador ou um colega de trabalho.
- A conformidade é um comportamento baseado em grupo, mas pode ser usado ocasionalmente no campo individual, convencendo o utilizador de que todos deram a informação ao atacante. Quando o atacante atacar e for feita uma investigação, o funcionário estará seguro pois pensa que todos estão implicados como ele.

A Vertente da Engenharia Social

Área de Risco	Atacante	Estratégia de Prevenção
HelpDesk	Persuasão e Personificação	Não divulgar passwords ou outra informação confidencial pelo telefone
Entrada em instalações	Acesso físico não autorizado	Vigilância de identificação
Escritório	Olhar sobre o ombro de um colaborador. Circular à procura de secretárias vazias. Roubo de informação sensível.	Não introduzir passwords com alguém ao lado. Acompanhar visitas diretamente à saída. Marcar documentação como confidencial e fechar os mesmos documentos.
Sala de Correio	Inserção de avisos falsos	Fechar e vigiar sala de Correio
Sala de Servidores	Tentativa de ganhar acesso para remover equipamento ou roubar dados confidenciais	Fechar sala dos telefones, o Datacenter e manter um inventário atualizado do equipamento
Telefone	Roubar acessos telefónicos	Controlar chamadas de longa distância e rastrear chamadas
Lixo	Remexer o lixo	Manter o lixo em áreas seguras e vigiadas, destruir dados confidenciais
Intranet / Internet	Criação e inserção de software de roubo e rastreio de password na rede	Mudanças contínuas na sensibilização da rede
Geral	Personificação e persuasão	Manter os funcionários informados e com formações sobre o problema

A Vertente da Engenharia Social

- Alguns pontos fundamentais na proteção contra ataques de engenharia social:
  - Limitar o número de contas de utilizadores com privilégios na organização e o nível de acesso que eles têm, isso irá ajudar a limitar o dano que um ataque de engenharia social bem-sucedido possa causar.
  - Regularmente rever as contas dos utilizadores. Fornecer acessos apenas para os que devem ter acesso e os recursos específicos para quem realmente precisa.
  - Verificar se as contas de utilizador têm uma autenticação forte.

Mecanismos de proteção e técnicas de defesa

- Ataque Buffer-OverFlow
  - Os buffer-overflows são a ameaça de segurança mais comum em sistemas de software hoje em dia e muitas da vulnerabilidades existentes devem-se a buffer-overflows (B.O). Qualquer mitigação desta vulnerabilidade iria ter um grande impacto na melhoria da segurança das nossos máquinas e sistemas.

- Mecanismos de proteção e técnicas de defesa
  - Os detetores de buffer overflow estáticos tentam verificar se todos os acessos à memória sofrem de overflow. Ferramentas inadequadas e mal configuradas, levam a perda de erros no código.

  - Estes detetores são interessantes pois inserem automaticamente as proteções necessárias. Mas para um detector dinâmico ser implementado é fundamental que a proteção de buffer overflow, não quebre código de trabalho, ou seja deve ser feita automaticamente, sem intervenção do utilizador e seja razoavelmente eficaz.

Mecanismos de proteção e técnicas de defesa

- Ataque Race Condition
  - Nos sistemas operativos, os processos que correm juntos partilham um espaço de memória, em que cada um pode ler ou escrever. Uma corrida ocorre quando numa aplicação é possível infringir um pressuposto, desta forma violando a ordem de um procedimento previamente programado. Denomina-se por janela de vulnerabilidade ao intervalo de tempo que permite fazer essa infração.
  - Um exemplo de uma corrida pode ocorrer no print spooler.

- Mecanismos de proteção e técnicas de defesa
  - Na maioria do tempo, um processo está ocupado a fazer computação interna que não leva a corridas, mas quando o processo precisa de aceder a memória partilhada, este entra na região critica.
  - De modo a reduzir o risco de corridas devem ser adoptadas algumas regras:
    - Dois processos não podem estar simultaneamente na sua região critica
    - Não se devem fazer suposições sobre a velocidade ou número de CPU's
    - Nenhum processo fora da sua região crítica pode bloquear outro
    - Nenhum processo deve esperar eternamente para entrar na sua zona crítica

Mecanismos de proteção e técnicas de defesa

- DLL Injection
  - Esta é uma técnica que utiliza o espaço de endereçamento de um processo para executar código e esse código obriga o processo a carregar uma DLL.

- Mecanismos de proteção e técnicas de defesa
  - Ao trabalhar com uma entrada não confiável, lembre-se que pode carregar código não confiável.
  - Não carregue DLLs não confiáveis da entrada de um utilizador.
  - Instalar analisadores.

Mecanismos de proteção e técnicas de defesa

- Controlos de Acesso
  - O mecanismo de controlo de acessos mais conhecido por Access Control List, ou ACL é uma lista com a identidade de um utilizador e as suas permissões sobre o recurso a aceder.
    - Discretionary access control lists (DACLs)
      - As DACLs identificam os utilizadores aos quais está atribuído ou negado o acesso a determinado recurso.
      - Se a DACL não identificar explicitamente um utilizador ou grupo onde o utilizador esteja incluído, o acesso ao recurso é negado.
      - Por omissão a DACL é controlada pelo utilizador que criou o recurso.
    - System access control lists (SACLs)
      - As SACLs identificam os utilizadores ou grupos que devem ser auditados quando acedem com ou sem sucesso ao recurso.
      - A auditoria é utilizada para monitorizar os eventos relacionados com os sistema ou com a segurança da rede, de modo a encontrar falhas de segurança e determinar a extensão e localização do problema.
      - Por omissão as SACL é controlada pelo utilizador que criou recurso.

Mecanismos de proteção e técnicas de defesa

- Outro dos problemas atuais deve-se ao facto de muitos dos utilizadores não perceberem que o seu computador/máquina pode ficar infetado com apenas uma visita a um website aparentemente legitimo.

- No entanto mais de 80% dos URLs maliciosos são sites legítimos que foram adulterados por hackers.

- Isto é conseguido através da exploração de vulnerabilidades no software ou por roubar credenciais de acesso a máquinas infectadas por malware.

Modelos de Segurança

- Os modelos de segurança fornecem um suporte para o desenvolvimento de técnicas para descrever e verificar a segurança dos sistemas informáticos.

- Modelo Bell-LaPadula
  - O modelo Bell-LaPadula deve-se aos cientistas David Bell e Leonard LaPadula que desenvolveram o modelo na década de 70. O modelo é fundamentado nos procedimentos de manipulação de informação em áreas ligadas à segurança americana.
  - O objetivo deste modelo é acrescentar meios de controlo de acesso obrigatório aos controlos de acesso discricionário. Definir controlos de acesso discricionário utilizando políticas de segurança que impeçam a passagem de informação de um nível de segurança superior para um nível inferior.
  - Este modelo destaca a confidencialidade e está fundamentado na categorização dos elementos de segurança, que definem o meio de acesso ao sistema. As informações são classificadas segundo quatro níveis hierárquicos de sensibilidade: não-classificada • confidencial • secreta • ultra-secreta.

Modelos de Segurança

- Modelo Biba
  - A motivação para se criar o modelo obrigatório Biba foi a preservação da integridade de um sistema, prevenir a modificação não autorizada de dados e manter a consistência dos mesmos.
  - No modelo Biba são definidas regras onde um utilizador que se encontre num nível de integridade mais elevado não pode ler um objeto que esteja num nível de inferior ao seu (NRD - No Read Down). Também estabelece o inverso, ou seja um utilizador que esteja num nível inferior de integridade não poderá escrever num objeto de um nível de integridade superior ao seu (NRU – No Write Up).

Níveis de Segurança

- Orange Book
  - Perante o aumento da consciencialização da segurança em sistemas surgiu a necessidade de quantificar a segurança e avaliar a confiança de um sistema.
  - Foi então publicado pelo governo americano o "Trusted Computer System Evaluation Criteria", ou "Orange Book" como ficou conhecido devido à capa ser laranja.

Níveis de Segurança

- Common Criteria
  - Para refletir a crescente evolução das tecnologias e reconhecimento de um mercado de TI, um conjunto de países desenvolveu um projeto para avaliar a segurança. O projeto ficou conhecido como CC (Common Criteria).
  - A certificação Common Criteria adotada em 1999, fornece algum nível de garantia de segurança, entre outras coisas permitindo aos utilizadores aplicar uma série de requisitos de avaliação aos seus produtos.
  - Apesar das certificações, os produtos não estão garantidamente livres de vulnerabilidades, mas garante um nível elevado de confiança, em como o produto funciona como documentado e que o fabricante fornecerá atualizações para eventuais falhas que sejam detetadas.

Caracterização do ambiente: Ataque e Defesa

Ataque	Defesa
Muito atrativo	Amplos recursos para desenvolver: Ferramentas Processos Procedimentos
Baixo Custo	
Subornar Criar informações falsas Manipular informação Utilização de armas lógicas	Custo elavado
	Limites Tecnológicos
Lançada de qualquer parte do mundo	Limites Humanos
Não deixa rasto	Não se consegue antecipar a tudo
Tecnologia gratuita na Internet	A ameaça interna

QUESTÕES

?