Principais Ameaças e Vulnerabilidades

Kalinka Regina Lucas Jaquie Castelo Branco

Slides baseados nos slides do prof. Gleyson Azevedo, profa. Luciana Martimiano, CERT.BR, entre outros.

Introdução

Vulnerabilidade – **falha** no **projeto**, **implementação** ou **configuração** de **software** ou **sistema operacional** que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Um software ou sistema operacional pode conter uma vulnerabilidade que permite sua exploração remota através da rede.

Nesse caso, um atacante conectado à Internet, ao explorá-la, pode obter **acesso não autorizado** ao computador vulnerável.

Introdução – Tipos de Ataque

- Obtenção de Informações
  - Engenharia Social
  - Phishing
  - Packet Sniffing
  - Firewalking
  - Port Scanning
  - Scanning de Vulnerabilidades
  - IP Spoofing

Introdução – Tipos de Ataque

- Códigos Maliciosos (Malware)
  - Vírus
  - Cavalos de Troia
  - Adware e Spyware
  - Backdoors
  - Keyloggers e Screenloggers
  - Worms
  - Bots e Botnets
  - Rootkits
- Negação de Serviço (DoS) e Ataques coordenados (DDoS)

Obtenção de Informações - Engenharia Social

Método de ataque onde alguém faz uso da **persuasão**, explorando a **ingenuidade** ou a **confiança** do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Exemplo 1: ligação de desconhecido que diz ser do suporte técnico do provedor de Internet. Ele diz que a conexão está apresentando algum problema e pede a senha do cliente para corrigi-lo. Caso seja entregue, ele poderá realizar uma infinidade de atividades maliciosas, utilizando a conta de acesso à Internet do cliente e, portanto, relacionando tais atividades ao nome dele.

Obtenção de Informações - Engenharia Social

Exemplo 2: mensagem de e-mail, dizendo que o computador está infectado por vírus. Ela sugere a instalação de uma ferramenta disponível em um site para desinfecção. A real função da ferramenta não é eliminar um vírus, mas permitir que alguém tenha acesso ao computador e a todos os dados nele armazenados.

Exemplo 3: mensagem de e-mail, onde o remetente é o gerente ou o departamento de suporte do banco de um cliente. Ela diz que o serviço de Internet Banking está apresentando um problema que pode ser corrigido se for executado o aplicativo anexado à mensagem. A execução do aplicativo apresenta uma tela análoga a utilizada para ter acesso à conta bancária pela digitação da senha. Este aplicativo está preparado para furtar a senha de acesso à conta bancária e enviá-la para o atacante.

Obtenção de Informações - Engenharia Social

Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados nos exemplos procuram induzir o usuário a realizar alguma tarefa e o sucesso do ataque depende única e exclusivamente da decisão do usuário em fornecer informações sensíveis ou executar programas.

8

Ataques tipo "força bruta"

- Coletam dados do usuário (nomes, datas, telefones, etc).
- Elaboram combinações entre estes dados.
- Para cada combinação produzida, uma tentativa de acesso é realizada.
  - Facilmente combatidos com limites de tentativas e *captchas*.

8

Bombas Lógicas

- Um dos mais velhos aplicativos maliciosos, precedendo os vírus e *worms*
- Código embutido em programas legítimos que quando certas condições forem atingidas ele "explode"
  - Data específica
  - presença ou falta de arquivos
  - determinado usuário que esteja rodando a aplicação
- Quando é disparada, pode apagar e alterar ou remover dados ou arquivos inteiros, causar uma pane na máquina ou algum outro dano

Como se proteger ?

Obtenção de Informações - Phishing

Phishing – tipo de fraude que se dá por meio do envio de mensagem não solicitada, passando-se por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários. Também conhecido como phishing scam ou phishing/scam.

A palavra phishing (de "fishing") vem de uma analogia criada pelos fraudadores, onde "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

9

Obtenção de Informações - Phishing

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;

mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

10

Obtenção de Informações - Phishing

Principais situações envolvendo phishing:

mensagens que contêm links para programas maliciosos;

páginas de comércio eletrônico ou Internet Banking falsificadas;

e-mails contendo formulários para o fornecimento de informações sensíveis;

comprometimento do serviço de resolução de nomes (DNS).

11

Obtenção de Informações – Packet Sniffing

Técnica que consiste na captura de informações valiosas diretamente pelo fluxo de pacotes. Também conhecida como *passive eavesdropping*.

Sniffer – dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores.

Há diversos softwares com essa capacidade, como o tcpdump, fornecido com o Linux, o Ethereal e o Wireshark.

12

Obtenção de Informações – Packet Sniffing

As informações capturadas pelos sniffers dizem respeito aos pacotes que trafegam no mesmo segmento de rede em que o aplicativo se encontra.

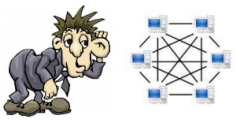
Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Há diversas técnicas que podem ser empregadas na detecção remota de sniffers: requisição ICMP com falso MAC, requisição ARP com falso MAC, DNS reverso, Latência, dentre outras.

13

Obtenção de Informações – Packet Sniffing

- Atividade maliciosa onde o atacante se conecta a uma LAN por exemplo, e passa a "escutar" os dados que trafegam nos canais de comunicação.
    - Dados não protegidos podem ser capturados.



13

Exercícios

1. (Perito Criminal – Processamento de Dados – CPC/PA/2007 - CESPE) [31] Quanto ao monitoramento de tráfego em uma rede, julgue os seguintes itens.

I O tcpdump é um *packet sniffer* que possibilita a interceptação e apresentação de pacotes que trafegam por uma rede TCP/IP. Os dados nos pacotes interceptados podem ser armazenados em arquivos para posterior análise.

II Um *packet sniffer* possibilita monitorar o tráfego em uma rede. Em uma rede Ethernet, para monitorar o tráfego destinado ao endereço de broadcast, a placa de interface com a rede precisa ser configurada no modo promíscuo.

III Em uma rede Ethernet, um *packet sniffer* pode ser usado para monitorar o tráfego destinado ao endereço de broadcast e a endereços de *multicast*, mas não tráfego *unicast* destinado à máquina com o *packet sniffer*.

IV Há técnicas que podem ser usadas para se tentar identificar a presença de *packet sniffers* em redes Ethernet. Por exemplo, um pacote ARP pode ser enviado para um endereço que não seja o de broadcast. Se uma máquina responder a esse pacote, possivelmente tem uma placa de rede no modo promíscuo.

Estão certos apenas os itens

A. I e II. B. I e IV. C. II e III. D. III e IV.

14

Exercícios

2. (Perito Criminal Federal – Computação Científica – PF/2002 - CESPE) [44] Considere uma rede em que há a suspeita da existência de um *sniffer* instalado em uma das máquinas que compõem a rede, realizando escutas desautorizadas. Com relação a essa situação, julgue os itens abaixo.

1 [1] Constitui boa estratégia de detecção de *sniffer* aquela que se fundamenta na identificação do tráfego gerado por ele durante a escuta, tráfego que normalmente acontece em grande quantidade, seja o *sniffer* em redes comutadas ou não.

2 [2] Pode-se detectar a existência de um *sniffer* na rede usando-se outro *sniffer* e verificando quem faz consultas de DNS quando uma nova máquina é adicionada à rede.

3 [3] Na identificação de um *snnifer*, constitui boa estratégia o envio de pings em broadcast e a comparação dos tempos de resposta das várias máquinas no segmento: o tempo de resposta da máquina que contém *sniffer* provavelmente será maior que o das outras máquinas.

4 [4] Um *sniffer* comum — passivo — em uma rede comutada consegue capturar tráfego.

5 [5] A detecção de um *sniffer* quase sempre acontece com sucesso, sendo a sua identificação fundamentada no endereço MAC.

15

Exercícios

3. (Perito Criminal Federal – Computação Científica – PF-Nacional/2004 – CESPE) Acerca das vulnerabilidades e proteções dos sistemas de informação, julgue o item a seguir.

1 [99] A captura de pacotes que trafegam na rede com uso de um sniffer é um exemplo de ataque para o qual não há nenhuma forma de detecção possível pelo administrador de rede.

16

Obtenção de Informações – Firewalking

O firewalking é uma técnica implementada em uma ferramenta similar ao traceroute e pode ser utilizada para obtenção de informações sobre uma rede remota protegida por um firewall.

Essa técnica permite que pacotes passem por portas em um gateway, além de determinar se um pacote com várias informações de controle pode passar pelo gateway.

Pode-se ainda mapear roteadores encontrados antes do firewall.

Pode-se obter informações sobre as regras de filtragem e também criar um mapa da topologia da rede.

17

Obtenção de Informações – Scan

- Programas (*scanners)* que descobrem os *hosts* de uma rede.
- Para cada *host*, fazem um conjunto de verificações para descobrir possíveis vulnerabilidades de S.O.s ou de aplicações.

17

Exploração de falhas em aplicações e S.O.s

- "Todo software está sujeito a falhas".
- Ataques que exploram exclusivamente vulnerabilidades existentes ou falhas de configuração de *softwares*.

17

Obtenção de Informações – Port Scanning

Port Scanners – são ferramentas utilizadas para obtenção de informações referentes aos serviços que são acessíveis e definidas por meio do mapeamento das portas TCP e UDP.

O intuito desse tipo de ataque é evitar o desperdício de esforço com ataques a serviços inexistentes.

O nmap é um dos port scanners mais utilizados e pode ser empregado para realizar a auditoria do firewall e do IDS.

18

Obtenção de Informações – Scanning de Vulnerabilidades

Após a identificação dos sistemas que podem ser atacados e dos serviços que são executados, deve-se proceder à procura pelas vulnerabilidades existentes, o que deve ser feito por um scanner de vulnerabilidades.

Scanners de Vulnerabilidades – são ferramentas que realizam diversos tipos de testes na rede, à procura de falhas de segurança, seja em protocolos, serviços, aplicativos ou sistemas operacionais.

O mapeamento anteriormente feito pelo port scanning é importante porque a busca de vulnerabilidades pode ser realizada especificamente para o que foi mapeado.

19

Obtenção de Informações – Spoofing

Spoofing – ataque onde o sujeito autentica um host para outro se utilizando da técnica de forjar pacotes originários de um host confiável.

Os principais e mais largamente utilizados tipos de spoofing são:

IP Spoofing;

ARP Spoofing;

DNS Spoofing.

20

Spoofing – IP

Muitos serviços que utilizam o protocolo TCP/IP funcionam às custas de um tipo de autenticação baseada em hosts (address-based authentication).

Assim, a autenticação para um determinado serviço é feita pela simples verificação do hostname e/ou IP do solicitante em uma lista de "hosts confiáveis".

Se houver relação, o solicitante estará autorizado a utilizar o serviço, do contrário, não.

Todavia, o spoofing não é tão simples assim. O fato de se alterar o IP da origem não torna o spoofing possível, pois há outras condicionantes, entre as quais a mais importante é como são gerenciadas as conexões e transferências TCP.

21

Spoofing – IP

Para que haja uma conexão entre dois hosts existem uma série de checagens passadas de lado a lado até que a conexão seja definitivamente estabelecida.

Por esta razão, o TCP se utiliza de uma seqüência de números, associando-os aos pacotes como identificadores, que são utilizados por ambos os hosts para checagens de erros e informe destes, de maneira que ao ser iniciada a conexão, o host solicitante envia um pacote TCP com uma seqüência de números inicial.

22

Spoofing – IP

O servidor responde então com sua seqüência de números e um ACK. Esta seqüência é igual a do cliente + 1. Quando o solicitante ou cliente recebe o ACK do servidor ele envia então o seu, que trata-se da seqüência enviada inicialmente pelo servidor + 1.

A pessoa que irá realizar o spoofing tem então dois problemas na verdade: o de alterar o IP origem, mais simples de resolver, e o de manter a seqüência de números, que por serem geradas arbitrariamente, complica em muito esta tarefa.

23

Spoofing – IP

Existe uma infinidade de ferramentas para facilitar esta tarefa, que, em sua maioria, são programas que analisam as seqüências e tentam obter uma lógica qualquer entre os números.

Como exemplo, tem-se o spoofit, o mendax, o seq_number, o ipspoof e outros, todos em C, o que significa que podem ser executados em várias plataformas, dependendo apenas de uma compilação correta.

24

Spoofing – IP

A vulnerabilidade a este ataque varia de sistema pra sistema, sendo mais ou menos efetiva de acordo com o algoritmo utilizado para a geração das seqüências numéricas e o número de serviços rodando que se utilizam de autenticação address-based, condenada há muito, pelo menos desde 1985, de acordo com o artigo publicado de Robert Morris, então da Bell Labs.

Ainda assim, há uma infinidade de servidores contendo inúmeros serviços que se utilizam de RPC (Remote Procedure Call), sabidamente vulneráveis a ataques do tipo IP spoofing.

25

Spoofing – ARP

Spoofing ARP – variação do IP spoofing que se aproveita do mesmo tipo de vulnerabilidade (também é address-based), diferenciando-se apenas por utilizar o endereço físico ou MAC (Media Access Control).

O host atacante envia um mapa com informações erradas ao ARP cache remoto, de maneira que os pacotes que saem do alvo para o seu suposto destino são roteados para o host que atacou.

Este ataque tem uma série de limitações, sendo uma delas o tempo em que uma entrada dinâmica permanece no ARP cache, que é muito curto, desfazendo então a informação errada inicialmente implantada.

26

Envenenamento de DNS

- O que é DNS?
  - Domain Name Server
  - Dispositivo de Internet são localizados por números únicos (IPs).
  - Números são difíceis de se memorizar, porque não associá-los a nomes?
- Servidor DNS
  - Entidade que mantém uma tabela de associação Entre nomes e números que identificam computadores (serviços) na Internet.
  - Funciona como uma espécie de agenda de telefone.

27

Envenenamento de DNS

- É uma fraude na associação entre os nomes e os identificadores dos computadores/serviços na Intenet.
  - Ex. um *host* está em uma rede que "sofre" de envenenamento de DNS pode ser redirecionado para uma página fraudulenta quando solicitar o identificador de www.bancodobrasil.com.br para um servidor DNS.

27

Spoofing – DNS

Esta técnica é muito simples e não requer grandes conhecimentos do TCP/IP.

Consiste em se alterar as tabelas de mapeamento de host name – IP address dos servidores DNS, de maneira que os servidores, ao serem perguntados pelos seus clientes sobre um hostname qualquer, informam o IP errado, ou seja, o do host que está aplicando o DNS spoofing.

27

Exercícios

4. (Perito Criminal Federal – Computação Científica – PF-Nacional/2004 – CESPE) Acerca das vulnerabilidades e proteções dos sistemas de informação, julgue o item a seguir.

1 [98] Um ataque de scanner consiste na monitoração de serviços e versões de software que estão sendo executados em um determinado sistema. Um sistema firewall que implementa um filtro de conexões é capaz de anular os efeitos desse tipo de ataque.

5. (Analista Judiciário – Informática – STJ/2008 - CESPE) Com respeito a vulnerabilidades e ataques a sistemas computacionais, julgue o item que se segue.

1 [109] Em redes IP que utilizam switches, pode-se realizar a escuta do tráfego com o ARP spoofing.

28

Exercícios

6. (Analista de Controle Externo – Tecnologia da Informação – TCU/2008 - CESPE) Julgue o item abaixo, relativo à segurança da informação.

1 [174] Em caso de ataques do tipo e-mail *spoofing* aos usuários da rede, recomenda-se que o administrador da rede adote o uso de certificados do tipo X.509, o qual permitirá aos destinatários identificarem corretamente os e-mails recebidos.

7. (Técnico Científico – Banco da Amazônia/2006 - CESPE) No tocante a vulnerabilidades, mecanismos, técnicas e políticas de segurança em redes, julgue o item a seguir.

1 [112] Um ataque de *spoofing* se baseia em uma situação na qual uma pessoa ou programa consegue se mascarar com sucesso, por exemplo, se fazendo passar por outra por meio de falsificação de dados. Um exemplo desse tipo de ataque vem da área de criptografia e é conhecido como *man in the middle attack*.

29

Exercícios

8. (Analista de Tecnologia da Informação – Redes – DATAPREV/2006 – CESPE) No referente a segurança de rede e controle de acesso, julgue os itens que se seguem.

1 [67] A restrição na capacidade de aprendizado de endereços nas portas de um *switch* é suficiente para evitar o ARP *spoofing*.

2 [69] Ataques ao STP (spanning tree protocol – IEEE 802.1D) podem potencializar ataques como o do MAC flooding e o do ARP spoofing.

30

Códigos Maliciosos (Malwares)

Código malicioso ou **Malware** (**Mal**icious Soft**ware**) – termo que abrange todos os tipos de programa especificamente desenvolvidos para executar **ações maliciosas** em um computador.

Exemplos:

- vírus;
- worms;
- backdoors;
- cavalos de tróia;
- keyloggers;
- rootkits.

31

Códigos Maliciosos (Malwares)

Classificações:

- dependência de hospedeiro:
  - dependentes (vírus, bombas lógicas e backdoors);
  - independentes (worms e zumbis).
- replicação:
  - não se replicam (bombas lógicas, backdoors e zumbis);
  - se replicam (vírus e worms).

32

Códigos Maliciosos - Vírus

Vírus – programa ou parte de programa que se **propaga infectando**, isto é, inserindo **cópias de si mesmo** e se tornando parte de **outros programas** e **arquivos** de um computador.

O vírus **depende** da **execução** do **programa ou arquivo hospedeiro** para que possa se tornar ativo e dar continuidade ao processo de infecção.

Entende-se por computador qualquer dispositivo computacional passível de infecção por vírus. Ex: desktops, notebooks, telefones celulares, PDAs dentre outros.

33

Códigos Maliciosos - Vírus

Normalmente o vírus tem controle total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de "feliz aniversário", até alterar ou destruir programas e arquivos do disco.

Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- abrir arquivos anexados aos e-mails;
- abrir arquivos do Word, Excel, etc;

34

Códigos Maliciosos - Vírus

(Cont.):

- abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, pen drives, CDs, DVDs, etc;
- ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele é ligado.

35

Códigos Maliciosos - Vírus

Existem **vírus** que procuram permanecer **ocultos**, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Ainda existem outros tipos que permanecem **inativos** durante certos períodos, entrando em atividade em datas específicas.

Vírus Propagado por E-mail

- um **vírus propagado por e-mail** (e-mail borne virus) normalmente é recebido como um arquivo anexado à uma mensagem de correio eletrônico.
- O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado.

36

Códigos Maliciosos - Vírus

Vírus Propagado por E-mail

Quando este tipo de vírus entra em ação, ele infecta arquivos e programas e envia cópias de si mesmo para os contatos encontrados nas listas de endereços de e-mail armazenadas no computador do usuário.

É importante ressaltar que este tipo específico de vírus **não é capaz de se propagar automaticamente**. O usuário precisa executar o arquivo anexado que contém o vírus, ou o programa leitor de e-mails precisa estar configurado para auto-executar arquivos anexados.

37

Códigos Maliciosos - Vírus

Vírus de Macro

Uma **macro** é um **conjunto de comandos** que são armazenados em alguns **aplicativos** e utilizados para **automatizar** algumas **tarefas repetitivas**. Ex: em um editor de textos, definir uma macro que contenha a seqüência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons de cinza.

Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros.

38

Códigos Maliciosos - Vírus

Vírus de Macro

Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

Existem alguns aplicativos que possuem **arquivos base** (modelos) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será.

39

Códigos Maliciosos - Vírus

Vírus de Macro

Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access, são os mais suscetíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e PostScript são menos suscetíveis, mas isso não significa que não possam conter vírus.

40

Exercícios

9. (Analista de Sistemas – Suporte de Infraestrutura – IPEA/2008 - CESPE) Acerca de segurança em redes, julgue os itens seguintes.

1 [84] Atualmente, a maioria dos vírus ainda é detectada por meio de assinaturas. A pesquisa por assinatura é variável conforme o antivírus. Dá-se o nome de falso positivo a um alarme falso gerado pelo antivírus, isto é, quando um erro na lista de definição faz que o programa marque arquivos limpos e seguros como infectados.

2 [117] Um vírus metamórfico faz mutação a cada infecção, podendo tanto mudar de comportamento quanto de aparência.

10. (Tecnologista Jr – MCT/2008 – CESPE) Julgue o item abaixo, acerca de segurança dos sistemas de informação computacional e das redes de comunicação.

1 [105] Um vírus de macrocomandos de uma aplicação, como, por exemplo, um editor de textos, é independente da plataforma computacional e dos sistemas operacionais.

41

Códigos Maliciosos – Cavalo de Tróia

42

Códigos Maliciosos – Cavalo de Tróia

Cavalo de tróia (trojan horse) – programa, normalmente recebido como um "presente" (um cartão virtual, um álbum de fotos, um protetor de tela, um jogo, etc), que além de executar funções para as quais foi aparentemente projetado, executa outras normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- instalação de keyloggers ou screenloggers;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;

43

Códigos Maliciosos – Cavalo de Tróia

(Cont.)

- inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador;
- alteração ou destruição de arquivos.

44

Códigos Maliciosos – Cavalo de Tróia

Por definição, o cavalo de tróia distingue-se de um vírus ou de um worm por **não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente**.

Normalmente um cavalo de tróia consiste em um único arquivo que necessita ser explicitamente executado.

Podem existir casos onde um cavalo de tróia contenha um vírus ou worm, mas mesmo nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou worm.

45

Códigos Maliciosos – Cavalo de Tróia

É necessário que o cavalo de tróia seja executado para que se instale em um computador.

Ele geralmente vem anexado a um e-mail ou está disponível em algum site na Internet na forma de cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, etc.

Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar backdoors, alterar informações, apagar arquivos ou formatar o disco rígido ou apenas exibirem uma mensagem de erro.

46

Códigos Maliciosos – Cavalo de Tróia

Muitas vezes, o cavalo de tróia pode instalar programas para possibilitar que um invasor tenha controle total sobre um computador.

Estes programas podem permitir que o invasor:

- tenha acesso e copie arquivos;
- descubra senhas digitadas pelo usuário;
- formate o disco rígido do computador, etc.

Normalmente o cavalo de tróia procura instalar, sem que o usuário perceba, programas que realizam uma série de atividades maliciosas.

47

Exercícios

11. (Técnico Científico – Banco da Amazônia/2006 - CESPE) No tocante a vulnerabilidades, mecanismos, técnicas e políticas de segurança em redes, julgue o item a seguir.

1 [109] Um *trojan* é um programa não-autorizado, embutido dentro de um programa legítimo, que executa funções desconhecidas e, provavelmente, indesejáveis. O programa alvo realiza a função desejada, mas, devido à existência de código não-autorizado dentro dele, também executa funções desconhecidas.

49

Códigos Maliciosos – Adware e Spyware

Adware (Advertising software) – tipo de software especificamente projetado para apresentar **propagandas**, seja através de um browser, seja através de algum outro programa instalado em um computador.

São normalmente incorporados a softwares e serviços, constituindo uma **forma legítima** de patrocínio ou retorno financeiro para quem desenvolve software livre ou presta serviços gratuitos. Exemplo: versão gratuita do Opera.

Spyware – termo utilizado para se referir a uma grande categoria de software que tem o objetivo de **monitorar atividades** de um sistema e **enviar as informações** coletadas para terceiros.

50

Códigos Maliciosos – Adware e Spyware

Existem adwares que também são considerados um tipo de spyware, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Os spywares, assim como os adwares, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

51

Códigos Maliciosos – Adware e Spyware

Algumas funcionalidades implementadas em spywares, que podem ter relação com o uso legítimo ou malicioso:

- monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- alteração da página inicial apresentada no browser do usuário;
- varredura dos arquivos armazenados no disco rígido do computador;
- monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;

52

Códigos Maliciosos – Adware e Spyware

(Cont.):

- instalação de outros programas spyware;
- monitoramento de teclas digitadas pelo usuário ou regiões da tela próximas ao clique do mouse;
- captura de senhas bancárias e números de cartões de crédito;
- captura de outras senhas usadas em sites de comércio eletrônico.

53

Códigos Maliciosos – Adware e Spyware

Estes programas quase sempre comprometem a privacidade do usuário e a segurança da máquina, dependendo das ações realizadas e de quais informações são monitoradas e enviadas para terceiros.

São exemplos de utilização legítima de spyware:

- uma empresa monitorar os hábitos de seus funcionários, desde que essa atividade esteja prevista em contrato ou nos termos de uso dos recursos computacionais da empresa;
- um usuário instalar um spyware para verificar se outras pessoas estão utilizando o seu computador de modo abusivo ou não autorizado.

54

Códigos Maliciosos – Adware e Spyware

Exemplos de utilização dissimulada e/ou maliciosa:

- um cavalo de tróia que instala um spyware juntamente com um keylogger ou screenlogger. O spyware monitora os acessos enquanto o usuário navega na Internet. Sempre que o usuário acessa determinados sites, o keylogger ou screenlogger é ativado para captura de senhas bancárias ou números de cartão de crédito;
- alguns adwares incluem componentes spyware para monitorar o acesso a páginas e direcionar propagandas. Se a licença de instalação do adware não diz claramente ou omite o monitoramento e o envio de informações, está caracterizado o uso dissimulado ou não autorizado.

55

Exercícios

12. (Perito Criminal Federal – Computação Científica – PF-Nacional/2004 – CESPE) Acerca das vulnerabilidades e proteções dos sistemas de informação, julgue o item a seguir.

1 [97] Os programas conhecidos como *spyware* são um tipo de *trojan* que tem por objetivo coletar informações acerca das atividades de um sistema ou dos seus usuários e representam uma ameaça à confidencialidade das informações acessadas no sistema infectado. Esses programas não são considerados como vírus de computador, desde que não se repliquem a partir de um sistema onde tenham sido instalados.

56

Códigos Maliciosos – Backdoors

Backdoor – programa que permite o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim.

É comum um atacante procurar garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na invasão.

Na maioria dos casos, também é intenção do atacante poder retornar sem ser notado.

57

Códigos Maliciosos – Backdoors

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Uma outra forma é a instalação de pacotes de software, tais como o Back Orifice e NetBus, da plataforma Windows, utilizados para administração remota. Se mal configurados ou utilizados sem o consentimento do usuário, podem ser classificados como backdoors.

58

Códigos Maliciosos – Backdoors

A existência de um backdoor **não depende necessariamente de uma invasão**.

Alguns dos casos onde não há associação com uma invasão são:

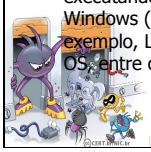
- instalação através de um cavalo de tróia;
- inclusão como conseqüência da instalação e má configuração de um programa de administração remota;
- alguns fabricantes incluem/incluíam backdoors em seus produtos (softwares, sistemas operacionais), alegando necessidades administrativas.

59

Códigos Maliciosos – Backdoors

Estes casos constituem uma séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que os backdoors tenham sido incluídos por fabricantes conhecidos.

Backdoors não são restritos a um sistema operacional específico, pois podem ser incluídos em computadores executando diversos sistemas operacionais, como Windows (por exemplo, 95/98, NT, 2000, XP), Unix (por exemplo, Linux, Solaris, FreeBSD, OpenBSD, AIX), Mac OS, entre outros.



60

Códigos Maliciosos – Keyloggers

Keylogger – programa capaz de capturar e armazenar a informação das teclas digitadas pelo usuário em um computador.

Dentre as informações capturadas podem estar um texto de e-mail, dados da declaração de imposto de renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site específico de comércio eletrônico ou Internet Banking.

61

Códigos Maliciosos – Keyloggers

Normalmente, o keylogger contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de e-mail).

As instituições financeiras desenvolveram teclados virtuais para evitar que os keyloggers pudessem capturar informações sensíveis de clientes. Como resposta, foram desenvolvidos os screenloggers, que são capazes de:

- armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou
- armazenar a região que circunda a posição onde o mouse é clicado.

62

Códigos Maliciosos – Keyloggers

Normalmente, o keylogger vem como parte de um programa spyware ou cavalo de tróia.

Desta forma, é necessário que este programa seja executado para que o keylogger se instale em um computador.

Geralmente, tais programas vêm anexados a e-mails ou estão disponíveis em sites na Internet.

63

Códigos Maliciosos – Screenlogger

- Programas capazes de escutar, salvar e compartilhar o Estado total ou parcial da tela (*printscreen*).
  - A partir de cliques, por exemplo;
  - Utilizado para driblar os teclados virtuais.

63

Códigos Maliciosos – Worm

Worm – programa capaz de **se propagar automaticamente através de redes**, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm **não** embute cópias de si mesmo em outros programas ou arquivos e **não** necessita ser explicitamente executado para se propagar.

Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

64

Códigos Maliciosos – Worm

Geralmente, o worm não tem como conseqüência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Worms são notadamente responsáveis por **consumir** muitos **recursos**. Degradam sensivelmente o **desempenho** de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.

65

Códigos Maliciosos – Bots e Botnets

Bot – programa capaz se propagar automaticamente (modo similar ao *worm*), explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.

Adicionalmente ao worm, dispõe de **mecanismos de comunicação com o invasor**, permitindo que o bot seja **controlado remotamente**.

Normalmente, o bot se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado, onde aguarda instruções do invasor monitorando, paralelamente, as mensagens que estão sendo enviadas para este canal.

66

Códigos Maliciosos – Bots e Botnets

O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo bot.

Estas sequências correspondem a instruções que devem ser executadas pelo bot.

67

Códigos Maliciosos – Bots e Botnets

Um invasor, ao se comunicar com um bot, pode enviar instruções para que ele realize diversas atividades, tais como:

- desferir ataques na Internet;
- executar um ataque de negação de serviço;
- furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
- enviar e-mails de phishing;
- enviar spam.

68

Códigos Maliciosos – Bots e Botnets

Botnets – redes formadas por computadores infectados com bots.

Podem ser compostas por centenas ou milhares de computadores.

Um invasor que tenha controle sobre uma botnet pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar milhares de e-mails de phishing ou spam, desferir ataques de negação de serviço, etc.

69

Códigos Maliciosos – Bots e Botnets

Identificar a presença de um bot em um computador não é uma tarefa simples.

Normalmente, o bot é projetado para realizar as instruções passadas pelo invasor sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de bots, isto nem sempre é possível.

70

Exercícios

13. (Analista de Controle Externo – Auditoria de TI – TCU/2007 - CESPE) Julgue o próximo item acerca dos conceitos de segurança da informação.

1 [153] São características típicas dos *malwares*: cavalos de tróia aparentam realizar atividades úteis; *adwares* obtêm e transmitem informações privadas do usuário; *backdoors* estabelecem conexões para fora da rede onde se encontram; *worms* modificam o código de uma aplicação para propagar-se em uma rede; e *botnets* realizam ataques articulados por meio de um controle remoto.

14. (Tecnologista Jr – MCT/2008 – CESPE) Julgue o item abaixo, acerca de segurança dos sistemas de informação computacional e das redes de comunicação.

1 [104] O verme (*worm*) computacional Nimda é capaz de se propagar utilizando múltiplos mecanismos, como correio eletrônico, áreas de compartilhamento de aplicações distribuídas, exploração de falhas em servidores do *hypertext transfer protocol* (HTTP) e acesso de portas de entrada escondidas em sistemas operacionais.

71

Códigos Maliciosos – Rootkits

Rootkit – conjunto de programas que fornece mecanismos para que um invasor possa **esconder** e **assegurar** a sua **presença** no computador comprometido.

O nome rootkit **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) a um computador, mas sim para mantê-lo.

O invasor, após instalar o rootkit, terá acesso privilegiado sem precisar recorrer novamente aos métodos utilizados na invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

72

Códigos Maliciosos – Rootkits

Um rootkit pode fornecer ferramentas com as mais diversas funcionalidades, podendo ser citados:

programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os rootkits), tais como arquivos, diretórios, processos, conexões de rede, etc;

backdoors, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos rootkits);

programas para remoção de evidências em arquivos de logs;

73

Códigos Maliciosos – Rootkits

(Cont.):

sniffers, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, sem qualquer proteção de criptografia;

scanners, para mapear potenciais vulnerabilidades em outros computadores;

outros tipos de malware, como cavalos de tróia, keyloggers, ferramentas de ataque de negação de serviço, etc.

74

Códigos Maliciosos – Rootkits

Existem programas capazes de detectar a presença de um grande número de rootkits, mas isto não quer dizer que são capazes de fazê-lo para todos os disponíveis (principalmente os mais recentes).

Como os rootkits são projetados para ficarem ocultos, sua identificação é, na maioria das vezes, uma tarefa bem difícil.

75

Exercícios

15. (Analista de Controle Externo – Auditoria de TI – TCU/2007 - CESPE) Julgue o próximo item acerca dos conceitos de segurança da informação.

1 [154] *Rootkits* apresentam portabilidade entre plataformas e devem ser manuseados conforme os controles estabelecidos no capítulo relativo à aquisição, desenvolvimento e manutenção de sistemas de informação da NBR 17799.

76

SPAM

Termo usado para se referir a mensagens (não Necessariamente email) não solicitadas, mas geralmente enviadas para um grande número de pessoas.

São utilizados para propagar *malwares* ou páginas falsas (*phishing*) que copiam dados de usuários.

77

Negação de Serviço (DoS)

Negação de Serviço (Denial of Service - DoS) – o atacante utiliza **um computador** para tirar de operação um serviço ou computador(es) conectado(s) à Internet.

Exemplos deste tipo de ataque são:

- gerar uma sobrecarga no processamento de um computador, de modo que o usuário não consiga utilizá-lo;
- gerar um grande tráfego de dados para uma rede, ocasionando a indisponibilidade dela;
- Indisponibilizar serviços importantes de um provedor, impossibilitando o acesso de seus usuários.

77

Negação de Serviço (DoS)

DDoS (Distributed Denial of Service) – ataque de negação de serviço distribuído, ou seja, um **conjunto de computadores** é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Normalmente, procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

Um exemplo de ataque DDoS ocorreu no início de 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos sites de empresas de comércio eletrônico.

78

Negação de Serviço (DoS)

Cabe ressaltar que se uma rede ou computador sofrer um DoS, isto não significa que houve uma invasão, pois o objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadi-los.

No exemplo citado, as empresas não tiveram seus computadores comprometidos, mas ficaram impossibilitadas de vender seus produtos durante um longo período.

79

Exercícios

16. (Analista de Controle Externo – Tecnologia da Informação – TCU/2008 - CESPE) Julgue o item abaixo, relativo à segurança da informação.

1 [176] Considere que um dos *hosts* da rede de uma organização esteja sofrendo um ataque da classe de negação de serviço (*denial of service* – DoS) e que, visando identificar de forma mais precisa o ataque que o *host* está sofrendo, o administrador tenha constatado que há elevada razão entre o número de pacotes TCP do tipo SYN e o número de pacotes TCP do tipo ACK que estão sendo enviados para o *host* sob ataque e que, por outro lado, a razão entre o número de pacotes TCP do tipo SYN recebidos pelo *host* e o número de pacotes do tipo SYN/ACK enviados pelo *host* é aproximadamente igual a 1. Nessa situação, o administrador deverá considerar a possibilidade de o ataque sob análise ser do tipo SYN *flood*, visto que são reduzidas as chances de o ataque ser do tipo NAK/ACK.

80

Exercícios

17. (Analista de Sistemas – Suporte de Infraestrutura – IPEA/2008 - CESPE) Acerca de segurança em redes, julgue o item abaixo.

1 [118] Em um ataque negação de serviço por refletor — reflector distributed denial of service (DDoS) — entidades escravas do atacante constroem pacotes que requerem respostas e contém o endereço IP do alvo como endereço fonte no cabeçalho, de modo que ao serem enviados a computadores não infectados, os refletores, tais pacotes provocam respostas direcionadas ao endereço alvo do ataque.

18. (Tecnologista Jr – MCT/2008 – CESPE) Julgue o item abaixo, acerca de segurança dos sistemas de informação computacional e das redes de comunicação.

1 [106] A contramedida que consiste em varrer portas de servidores locais para descobrir serviços que estão indevidamente ativos é um dos modos efetivos de realizar o rastreamento e a identificação das fontes de ataque do tipo negação de serviço distribuído.

81

Exercícios

19. (Perito Criminal Federal – Computação Científica – PF-Regional/2004 – CESPE) Acerca da segurança fornecida em ambientes de redes, julgue o item a seguir.

1 [105] Um dos mais conhecidos ataques a um computador conectado a uma rede é o de negação de serviço (DoS – denial of service), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.

20. (Analista de Controle Externo – Auditoria de TI – TCU/2007 - CESPE) Julgue o próximo item acerca dos conceitos de segurança da informação.

1 [157] A detecção, por um *sniffer* de rede, de uma longa série de segmentos TCP SYN enviados de um host local para um host remoto, sem o correspondente envio de segmentos TCP ACK, sugere que a rede sob análise pode estar sofrendo um ataque de negação de serviço.

82

Exploits

- Um *exploit*, em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional – como o próprio sistema operacional ou serviços de interação de protocolos (ex: servidores Web).
- São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas. Por isso muitos crackers não publicam seus exploits, conhecidos como 0days, e o seu uso massificado deve-se aos script kiddies.
- Até meados dos anos 90, acreditava-se que os exploits exploravam exclusivamente problemas em aplicações e serviços para plataformas Unix. A partir do final da década, especialistas demonstraram a capacidade de explorar vulnerabilidades em plataformas de uso massivo, por exemplo, sistemas operacionais Win32 (Windows 9x, NT, 2000 e XP). Como exemplo temos o CodeRed, o MyDoom, o Sasser em 2004 e o Zotob em 2005.

Exploit Database - http://www.exploit-db.com/
Packet Storm - http://packetstormsecurity.org/
Computer Security Vulnerabilities - http://securityvulns.com/

83

Exemplos

Principais Anti-*Malwares*

- Anti-virus
- Anti-*spyware*
- Filtro Anti-*Span*

Anti-Virus

- Programa ou sofware especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos"

http://antispam.br/

Anti-*Spyware*

- Programa utilizado para combater *spyware* (*keyloggers, screenlogers* entre outros programas espiões).

Anti-*Span*

- Programa que utiliza mecanismos de detecção de mensagens indesejadas, além de permitir a separação dos *e-mails* conforme regras pré-definidas.

Referências Interessantes

- Open Web Application Security Project (OWASP) - http://www.owasp.org/
  - OWASP Top 10 - http://www.owasp.org/index.php/OWASP_Top_10
- Security Focus – http://www.securityfocus.com
- Cert.Br – http://www.cert.br
  - Práticas de Segurança para Administradores de Redes Internet - http://www.cert.br/docs/seg-adm-redes/
- Help Net Security - http://www.net-security.org/
- Sans.org – http://www.sans.org
  - Top Cyber Security Risks - http://www.sans.org/top-cyber-security-risks/
  - Top 25 Software Errors - http://www.sans.org/top25-software-errors/

Referências Interessantes

- STALLINGS, William. Network Security Essentials – Applications and Standards – 3rd Edition. Pearson. 2007
- PADRÃO ISO/IEC INTERNACIONAL 17799 - Tecnologia da Informação – Código de Prática para Gestão da Segurança de Informações
- Catálogo de fraudes (CAIS) - http://www.rnp.br/cais/fraudes.php
- Network Security History – http://web.mit.edu/~bdaya/www/Network%20Security.pdf
- Timeline of computer security hacker history - http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
- 10 Famous Hackers - http://curiosity.discovery.com/topic/internet-communications/10-famous-hackers-hacks1.htm
- Fóruns
  - Invaders - http://www.forum-invaders.com.br/vb/
  - Invasão - http://www.forum.invasao.com.br/