República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0809841-7 B1

(22) Data do Depósito: 16/04/2008

(45) Data de Concessão: 09/03/2021

(54) Título: MÉTODO, APARELHO E EQUIPAMENTO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM

(51) Int.Cl.: H04L 29/06.

(52) CPC: H04L 63/126; H04L 63/1458.

(30) Prioridade Unionista: 23/04/2007 US 11/738,547.

(73) Titular(es): INTERNATIONAL BUSINESS MACHINES CORPORATION.

(72) Inventor(es): SUSANN MARIE KEOHANE.

(86) Pedido PCT: PCT EP2008054617 de 16/04/2008

(87) Publicação PCT: WO 2008/128941 de 30/10/2008

(85) Data do Início da Fase Nacional: 23/10/2009

(57) Resumo: MÉTODO, APARELHO, EQUIPAMENTO E PRODUTO DE PROGRAMA DE COMPUTADOR PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM é um método implementado por computador, aparelhos e produtos programa de computador para varredura de proteção de portas. Um pacote de dados com uma resposta pela transmissão do cabeçalho do protocolo de controle é gerado para formar um pacote de dados pela resposta, em resposta à detecção de uma varredura de portas. O pacote de dados pela resposta ilícita será uma reposta de um receptor do pacote de dados modificada. A resposta de pacotes de dados é enviada para um primeiro endereço de protocolo de Internet associado com a varredura de portas. Um segundo endereço de protocolo de Internet é identificado a partir de um cabeçalho de resposta ao pacote de dados pela resposta. O endereço do segundo protocolo Internet é um endereço real de protocolo de Internet de uma fonte de varredura de porta. Todo o tráfego de rede a partir do segundo endereço protocolo de Internet pode ser bloqueada para prevenir um ataque a quaisquer portas abertas desde a origem da varredura de porta.

MÉTODO, APARELHO E EQUIPAMENTO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM

Campo da Invenção

[001] A presente invenção está relacionada em geral a um sistema de processamento de dados e, em particular a um método e aparelho para segurança de sistemas de processamento de dados. Mais particularmente, a presente invenção é dirigida a um método implementado por computador, aparelho e código de programa de computador utilizável por computador para bloquear uma varredura de porta usando origens falsas de endereços de protocolos da *Internet*.

Descrição da técnica relacionada

[002] Um usuário de um dispositivo de computação, tal como um cliente, conectado a uma rede pode executar uma aplicação ou outro serviço disponível em um dispositivo de computação diferente, como um servidor, através da ligação a uma porta no servidor associado com o aplicativo ou serviço. Uma porta é um ponto final de uma ligação lógica entre um cliente e um servidor em uma rede. As portas são normalmente identificadas por um número de porta. Cada aplicação disponível no servidor é associada a um número de porta diferente.

[003] Em outras palavras, uma porta é como uma porta ou portão de entrada para uma determinada aplicação em um computador. Como uma porta, uma porta pode ser aberta ou fechada. Uma porta aberta em um servidor é uma porta associada a um aplicativo que está atualmente

disponível no servidor para utilização por um ou mais computadores-clientes. Uma porta fechada é uma porta que não está associada a um aplicativo ou serviço que está disponível no servidor. Um hacker normalmente não pode acessar um computador através de uma porta fechada.

[004] Um dispositivo de computação pode acessar um determinado aplicativo em um servidor, especificando o número da porta associada com a aplicação específica. Usuários, no entanto, às vezes não autorizados ou mal-intencionados, podem querer acessar um aplicativo ou serviço no servidor para fins de lançar um ataque contra o servidor. Estes usuários geralmente são referidos como hackers ou crackers de computador. O servidor que é atacado por um hacker pode ser referido como uma vítima.

[005] Hackers geralmente não sabem que os aplicativos ou serviços estão disponíveis na vítima. Por isso, o hacker pode realizar uma varredura de portas. A varredura de portas é um método para a digitalização de forma sistemática das portas do computador para determinar quais portas são portas abertas associadas a um aplicativo disponível ou serviço e as portas que estão fechadas. Na porta de digitalização, de uma série de mensagens são enviadas solicitando uma conexão com cada porta conhecida. A resposta da vítima pretendida indica se a porta bem conhecido é uma porta aberta ou uma porta fechada. A varredura de portas é utilizada por hackers para instalar pontos de acesso aberto a um computador que pode ser vulnerável a um ataque.

[006] Uma vez que uma porta aberta fica vulnerável, um hacker pode lançar um ataque que pode fazer com que os recursos do aplicativo associado a porta aberta atacada fiquem indisponíveis para os usuários do aplicativo. Este tipo de ataque é por vezes referido como uma negação de serviço (DoS).

[007] Uma solução para este problema é fornecida por software de proteção de varredura de portas. Os softwares de proteção de varredura de portas identificam o endereço do protocolo de *Internet* da origem (IP) de uma solicitação de conexão que pode ser parte de uma varredura de portas. O software de proteção de varredura de portas, em seguida, bloqueia aquele

endereço IP de origem. Em outras palavras, o software de varredura de portas não permite que as mensagens adicionais daquele endereço IP de origem sejam recebidas. Isso pode impedir ataques subsequentes de um hacker usando o mesmo endereço de IP de origem.

[008] No entanto, os hackers têm contornado os atuais softwares de prevenção de varredura de portas usando um falso endereço IP de origem durante varreduras de porta para localizar portas abertas. Quando O software de varredura de portas reconhece que uma varredura de portas pode estar ocorrendo, o software de prevenção de varredura porta bloqueia o falso endereço de IP identificado nas mensagens de varredura de portas. No entanto, os softwares de prevenção de varredura de portas existentes não o verdadeiro endereço IP do hacker. Assim, o hacker permanece livre para lançar ataques em quaisquer portas abertas usando o endereço IP do hacker real, que não está bloqueado pelo software de prevenção de varredura de portas porta. Estes ataques podem levar às consequências de uma negação de serviço (DoS) sobre os usuários que tentam ganhar acesso legítimo a aplicações e/ou serviços prestados pela vítima. Além disso, estes ataques podem levar à perda de tempo, dados e receitas, enquanto os pedidos e/ou serviços não estiverem disponíveis.

SUMÁRIO DA INVENÇÃO

[009] As concretizações ilustrativas fornecem método implementado por computador, aparelho e programa de código utilizável por computador para varredura de portas de proteção. Em uma modalidade, o processo gera um pacote de dados de resposta com um cabeçalho modificado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados modificado de resposta em resposta à detecção de uma varredura de portas. Em uma modalidade, o cabeçalho modificado para um protocolo utilizado para

transmitir pacotes de dados é um cabeçalho modificado de controle de protocolo de transmissão.

[0010] O pacote de dados de resposta modificado obtém uma resposta de um receptor, ou destinatário, do pacote de dados modificado. O processo envia o pacote de dados para um primeiro endereço de encaminhamento associado a varredura de portas.

[0011] O processo identifica um segundo endereço de encaminhamento em um cabeçalho do pacote de dados de resposta em resposta ao recebimento de uma resposta ao pacote de dados de resposta modificado. O segundo endereço de encaminhamento é um endereço de encaminhamento verdadeiro de uma origem de varredura de portas. Todo o tráfego de rede do segundo endereço de encaminhamento pode então ser bloqueado para prevenir um ataque a quaisquer portas abertas. Em uma modalidade, o primeiro endereço de encaminhamento é um primeiro endereço de protocolo de *Internet* e o segundo endereço de encaminhamento é um segundo endereço de protocolo de *Internet*.

[0012] O cabeçalho modificado utilizado pelo protocolo para transmitir pacotes de dados pode incluir um número de sequência ruim. Um número de sequência ruim é um número de sequência que não se enquadra em um intervalo aceitável de números em sequência ou um protocolo que obtém uma resposta do destinatário do pacote de dados de resposta. Em outra concretização, o cabeçalho modificado pode incluir um sinalizador de redefinir ou um sinalizador de chegada. Em outra modalidade, o cabeçalho é gerado pela alteração de uma quantidade usada para gerar o pacote de dados de resposta modificado.

[0013] Visto de um primeiro aspecto, a presente invenção fornece um método de proteção de varredura de portas, o método compreendendo as etapas de: em resposta a detecção de uma varredura de portas, gerar um pacote de dados de resposta com um cabeçalho modificado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de

resposta modificado, onde o pacote de dados de resposta modificado obtém uma resposta de um destinatário do pacote de dados de resposta modificado; enviar o pacote de dados de resposta modificado para um primeiro endereço de encaminhamento associado à varredura de portas; e em resposta ao recebimento do pacote de dados de resposta modificado, identificar um segundo endereço de encaminhamento num cabeçalho da resposta, no qual o segundo endereço de encaminhamento é um endereço de encaminhamento verdadeiro de uma origem de varredura de portas.

[0014] Preferencialmente, a presente invenção fornece um método em que o cabeçalho modificado para o protocolo compreende um número de sequência que está fora de uma faixa aceitável de números de sequência.

[0015] Preferencialmente, a presente invenção fornece um método em que o número de sequência é uma violação do protocolo que irá obter uma resposta do destinatário.

[0016] Preferencialmente, a presente invenção fornece um método em que o cabeçalho modificado para o protocolo inclui um sinalizador de redefinir.

[0017] Preferencialmente, a presente invenção fornece um método em que o cabeçalho modificado para o protocolo inclui um sinalizador de chegada.

[0018] Preferencialmente, a presente invenção fornece um método em que a alteração do cabeçalho inclui ainda alterar uma quantidade usada para gerar o pacote de dados de resposta modificado.

[0019] Preferencialmente, a presente invenção fornece um método que compreende ainda a etapa de bloquear o tráfego de rede proveniente do segundo endereço de encaminhamento para evitar um ataque a quaisquer portas abertas.

[0020] Preferencialmente, a presente invenção fornece um método no qual o primeiro endereço de encaminhamento não é um endereço de encaminhamento correto de um dispositivo de computação.

[0021] Preferencialmente, a presente invenção fornece um método compreendendo ainda a etapa de - em resposta ao recebimento de um pacote de dados varredura de portas, identificar um endereço de encaminhamento de origem em um cabeçalho do pacote de dados de varredura portas como o primeiro endereço de encaminhamento.

[0022] Preferencialmente, a presente invenção fornece um método em que o cabeçalho modificado para o protocolo é um cabeçalho modificado de um protocolo de controle transmissão.

[0023] Preferencialmente, a presente invenção fornece um método em que o cabeçalho modificado para o protocolo é um cabeçalho modificado de um protocolo de datagrama do usuário.

[0024] Preferencialmente, a presente invenção fornece um método em que o primeiro endereço de encaminhamento é um primeiro endereço de protocolo da *Internet* no qual o segundo endereço de encaminhamento é um segundo endereço de protocolo da *Internet*.

[0025] Visto de um segundo aspecto, a presente invenção fornece um aparelho compreendendo: um sistema de barramento, um sistema de comunicação conectado ao sistema de barramento; uma memória conectada ao sistema de barramento, onde a memória com um programa de computador de código utilizável por computador; e uma unidade de processamento conectada ao sistema de barramento, onde a unidade de processamento do computador executa o código do programa utilizável por computador para gerar um pacote de dados de resposta com um cabeçalho modificado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta modificado em resposta à detecção de uma varredura de portas, onde o pacote de dados de resposta modificado obtém um pacote de dados de resposta de um destinatário do pacote de dados de resposta modificado; envia o pacote de dados de resposta modificado para a um primeiro endereço de encaminhamento associado com a varredura de portas; e identifica um segundo endereço de encaminhamento em um cabeçalho do

pacote de dados de resposta em resposta ao recebimento do pacote de dados de resposta, onde o segundo endereço de encaminhamento é um endereço de encaminhamento verdadeiro de uma origem de varredura de portas.

[0026] Preferencialmente, a presente invenção fornece um aparelho onde o cabeçalho modificado para o protocolo compreende um número de sequência, em que o número de sequência é um número sequencial que está fora de um intervalo de números de sequência aceitáveis.

[0027] Preferencialmente, a presente invenção fornece um aparelho onde o cabeçalho modificado para o protocolo inclui um sinalizador de redefinir.

[0028] Preferencialmente, a presente invenção fornece um aparelho onde o cabeçalho modificado para o protocolo inclui um sinalizador de chegada.

[0029] Preferencialmente, a presente invenção fornece um aparelho em que a unidade de processamento executa ainda o código de programa utilizável por computador para bloquear todo o tráfego de rede proveniente do segundo endereço de encaminhamento para evitar um ataque a quaisquer portas abertas.

[0030] Preferencialmente, a presente invenção fornece um aparelho onde o número de sequência é uma violação do protocolo que obtém uma resposta de um destinatário do pacote de dados de resposta.

[0031] Preferencialmente, a presente invenção fornece um aparelho onde o cabeçalho modificado para o protocolo é um cabeçalho modificado de protocolo de controle transmissão.

[0032] Preferencialmente, a presente invenção fornece um aparelho em que o primeiro endereço de encaminhamento é um primeiro endereço de protocolo da *Internet* e o segundo endereço de encaminhamento é um segundo endereço de protocolo da *Internet*.

[0033] Visto de um terceiro aspecto, a presente invenção fornece um sistema de proteção contra varreduras de portas, o sistema compreendendo um computador anfitrião, onde o computador anfitrião compreende:

um software reforçado de proteção para varreduras de portas para detectar uma varredura de portas e gerar um pacote de dados de resposta com um cabeçalho modificado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta modificado em resposta à detecção de uma varredura de portas; e um detector de endereço de protocolo da *Internet* de origem, onde detector de endereço de protocolo da *Internet* de origem a fonte de endereço de protocolo de *Internet* detector identifica um endereço de encaminhamento de origem em um cabeçalho de uma resposta ao pacote de dados de resposta modificado, no qual o endereço de encaminhamento da origem é um endereço de encaminhamento verdadeiro de uma origem de varredura de portas.

[0034] Preferencialmente, a presente invenção fornece um sistema onde o cabeçalho modificado para o protocolo inclui uma violação de protocolo para o desencadeamento de uma resposta de um destinatário do pacote de dados de resposta.

[0035] Preferencialmente, a presente invenção fornece um sistema onde o cabeçalho modificado para o protocolo com um sinalizador de redefinir ou um sinalizador de chegada.

[0036] Preferencialmente, a presente invenção fornece um sistema no qual o computador anfitrião é um primeiro computador e compreende ainda - um segundo computador, onde o segundo computador compreende um varredor de portas, onde o varredor de portas executa a varredura de portas no primeiro computador, através do envio de pacote de dados de varredura de portas contendo um endereço de encaminhamento de fonte falsa para o primeiro computador, onde endereço de encaminhamento da falsa origem não é um endereço de encaminhamento correto para o segundo computador e uma camada de protocolo de controle de transmissão/protocolo de *Internet*, onde a

camada de protocolo de controle de transmissão/protocolo de *Internet* gera a resposta ao pacote de dados de resposta modificado automaticamente.

[0037] Vista de um quarto aspecto, a presente invenção fornece um produto de programa de computador, carregável na memória interna de um computador digital, que inclui porções de código de software para a realização, quando dito produto for executado em um computador, de todas as etapas do método descrito acima.

[0038] Visto de um quinto aspecto o produto de programa de computador compreende: um meio utilizável por computador para proteção de varredura de portas, dito produto de programa de computador compreendendo - código de programa utilizável por computador para gerar um pacote de dados de resposta com um cabeçalho modificado para um protocolo usado para transmitir pacotes de dados para formar um pacote de dados de resposta modificado em resposta à detecção de uma varredura de portas, onde o pacote de dados de resposta modificado obtém um pacotes de dados de resposta de um destinatário do pacote de dados de resposta modificado; código de programa utilizável por computador para o envio de pacotes de dados de resposta modificado para um primeiro endereço de encaminhamento associado a varredura de portas e código de programa utilizável por computador para identificar um segundo endereço de encaminhamento em um cabeçalho do pacote de dados de resposta em resposta ao recebimento do pacotes de dados de resposta, onde o segundo endereço de encaminhamento é um endereço de encaminhamento verdadeiro de uma origem da varredura de portas.

[0039] Preferencialmente, a presente invenção fornece um produto de programa de computador onde o cabeçalho modificado para o protocolo compreende um número de sequência.

[0040] Preferencialmente, a presente invenção fornece um programa de computador onde o número de sequência é um número de sequência que não se enquadra em uma faixa aceitável de números de sequência.

[0041] Preferencialmente, a presente invenção fornece um método implementado por computador em que o número de sequência é uma violação do protocolo que irá obter uma resposta de um destinatário do pacote de dados de resposta.

[0042] Preferencialmente, a presente invenção fornece um produto de programa de computador onde o cabeçalho modificado para o protocolo inclui um sinalizador de redefinir.

[0043] Preferencialmente, a presente invenção fornece um produto de programa de computador onde o cabeçalho modificado para o protocolo inclui um sinalizador de chegada.

BREVE DESCRIÇÃO DOS DESENHOS

[0044] Concretizações da invenção são descritas abaixo em detalhes, apenas a título de exemplo, com referência aos desenhos que acompanham, em que:

[0045] A Figura 1 é uma representação pictórica de uma rede de sistemas de processamento de dados na qual as concretizações preferidas da presente invenção podem ser aplicadas;

[0046] A Figura 2 é um diagrama de blocos de um sistema de processamento de dados em que concretizações preferidas da presente invenção podem ser aplicadas;

[0047] A Figura 3 é um diagrama de blocos de um modelo de referência básica de uma interconexão de sistemas abertos (OSI), de acordo com uma concretização preferida da presente invenção;

[0048] A Figura 4 é um diagrama de blocos que ilustra um mecanismo de proteção de varredura de portas usado atualmente;

[0049] A Figura 5 é um diagrama de blocos que ilustra um fluxo através de um sistema de proteção para varredura de portas para detectar varredura de portas com um falso endereço de IP da origem, de acordo com uma concretização preferida da presente invenção;

[0050] A Figura 6 é um diagrama de blocos ilustrando um mecanismo de proteção de varredura de portas, de acordo com uma concretização preferida da presente invenção;

[0051] A Figura 7 é uma ilustração exemplar de pacotes de varredura de portas transmitidos durante uma varredura de portas de acordo com uma concretização preferida da presente invenção;

[0052] A Figura 8 é um fluxograma ilustrando um processo para a detecção de uma varredura de portas com um falso endereço de origem de IP, de acordo com uma concretização preferida da presente invenção, e

[0053] A Figura 9 é um fluxograma ilustrando um processo para modificar os pacotes de dados de resposta, de acordo com uma concretização preferida da presente invenção.

DESCRIÇÃO DETALHADA DA MODALIDADE PREFERIDA

[0054] Agora, com referência às Figuras e, em especial com referência às figuras 1-2, diagramas exemplares de ambientes de processamento de dados são fornecidos em que concretizações ilustrativas podem ser implementadas. Deve-se considerar que as figuras 1-2 são apenas exemplares e não se destinam a assegurar ou implicar qualquer limitação no que diz respeito aos ambientes em que concretizações diferentes podem ser aplicadas. Muitas alterações para os ambientes apresentados podem ser feitas.

[0055] Agora, com referência às figuras, a Figura 1 mostra uma representação pictórica de uma rede de sistemas de processamento de dados em que concretizações ilustrativas podem ser aplicadas. A rede de sistema de

processamento de dados 100 é uma rede de computadores em que concretizações podem ser aplicadas. A rede sistema de processamento de dados 100 contém a rede 102, que é o meio usado para fornecer ligações (links) de comunicações entre os vários dispositivos e computadores ligados entre si no sistema de processamento de dados 100 da rede. A rede 102 pode incluir conexões, como fios de cabos, ligações de comunicação sem fio ou cabos de fibra ótica.

[0056] No exemplo ilustrado, o servidor 104 e o servidor 106 se conectam a rede 102, juntamente com a unidade de armazenamento 108. Além disso, os clientes 110, 112 e 114 se conectam à rede 102. Esses clientes 110, 112 e 114 podem ser, por exemplo, computadores pessoais ou computadores de rede.

[0057] No exemplo ilustrado, o servidor 104 fornece dados, tais como arquivos de inicialização, imagens do sistema operacional e aplicativos para os clientes 110, 112 e 114. Os clientes 110, 112 e 114 são clientes para o servidor 104 neste exemplo. A rede do sistema de processamento de dados 100 pode incluir servidores, clientes e outros dispositivos adicionais não mostrados.

[0058] Um dispositivo de computação, tal como o cliente 110, pode executar uma aplicação ou outro serviço disponível em um dispositivo de computação diferente, como o servidor 106, disponível através da rede 102 por uma conexão em uma porta do servidor de 106 associado com a aplicação ou serviço desejado. Um aplicativo é um software de computador que usa os recursos de um dispositivo de computação para executar uma tarefa ou serviço para um usuário.

[0059] Uma porta é uma extremidade de uma conexão lógica entre o cliente 110 e o servidor 106 na rede 102. As portas são normalmente identificadas por um número de porta. Os números de porta vão de 0 a 65.536. Números de porta são atribuídos pela *Internet Assigned Numbers Authority* (IANA). A *Internet Assigned Numbers Authority* é operada pela *Internet Corporation for Assigned Names and Numbers* (ICANN).

[0060] Cada aplicação disponível no servidor 104 ou no 106 está associada a um número de porta diferente. Alguns números de porta são pré-atribuídos com base no tipo de aplicativo ou serviço que está associado a uma determinada porta. Esses números pré-atribuídos ou números padrão de porta são referidos como portas bem conhecidas. Há aproximadamente 1.024 números de porta bem conhecidos reservados ou pré-designados para determinados serviços e aplicações. Por exemplo, números de porta bem conhecidos incluem, mas não estão limitados a, a porta 80 para o tráfego do protocolo de transferência de hipertexto (HTTP), a porta 23 para a Telnet, a porta 25 para protocolo de transferência de correio simples (SMTP), a porta 53 para servidores de nome de domínio (DNS), e a porta 194 para o *Internet Relay Chat* (IRC). Assim, qualquer porta em qualquer servidor que for designado para o tráfego do protocolo de transferência de hipertexto terá tipicamente um número de porta atribuído de 80.

[0061] O cliente 110 pode acessar um determinado aplicativo no servidor 104 ou no 106 enviando uma solicitação de conexão que especifica o número da porta associada com a aplicação específica.

[0062] No exemplo descrito, o sistema de processamento dados 100 da rede de é a *Internet* com a rede 102 representando uma coleção mundial de redes e portais que usam a suite de protocolos *Transmission Control Protocol* / *Internet Protocol* (TCP / IP) para se comunicar um com o outro. No coração da *Internet* existe uma espinha dorsal linhas de comunicação de dados de alta velocidade entre os nós principais ou computadores anfitriões, composto de milhares de sistemas de computador comerciais, governamentais, educacionais e outros que encaminham os dados e as mensagens. Naturalmente, os dados da rede do sistema de processamento de 100 também pode ser implementado como um número de diferentes tipos de redes, como por exemplo, uma intranet, uma rede de área local (LAN) ou uma rede de área ampla (WAN). A Figura 1 destina-se, como exemplo, e não como uma limitação de arquitetura para concretizações diferentes.

[0063] Com referência agora à Figura 2, um diagrama de blocos de um sistema de processamento de dados é mostrado na qual concretizações ilustrativas podem ser aplicadas. O sistema de processamento de dados 200 é um exemplo de um computador, como o servidor de 106 ou o cliente 110 da Figura 1, em que o código utilizável por computador ou instruções que implementem os processos podem ser localizado para as concretizações ilustrativas.

[0064] No exemplo descrito, o sistema de processamento de dados 200 emprega uma arquitetura de hub, incluindo uma ponte norte e um hub controlador de memória (MCH) 202 e uma ponte sul e um hub controlador de entrada / saída (I/O) (ICH) 204. A unidade de processamento 206, a memória principal 208, e o processador de gráficos 210 são acoplados a ponte norte e ao hub controlador de memória 202. A unidade de processamento de 206 pode conter um ou mais processadores e pode até ser implementada usando um ou mais sistemas de processamento heterogêneo. Os processadores gráficos 210 podem ser acoplados ao MCH através de uma porta de gráficos acelerada (AGP), por exemplo.

[0065] No exemplo ilustrado, a rede de área local (LAN) 212 é acoplada a ponte sul e ao hub controlador de E/S 204 e ao adaptador de áudio 216, ao adaptador de teclado e mouse 220, ao modem 222, a memória só de leitura (ROM) 224, ao universal serial bus (USB) e a outras portas de comunicação 232, e dispositivos PCI / PCIe 234 são acoplados a ponte sul e ao hub controlador de E/S (I/O) 204 pelo barramento 238, e unidade de disco rígido (HDD) 226 e CD-ROM 230 são acoplados a ponte sul e ao hub controlador de E/S (I/O) 204 pelo barramento 240. Dispositivos PCI/PCIe podem incluir, por exemplo, placas Ethernet, placas de expansão, e cartões de PC para computadores portáteis. Dispositivos PCI utilizam um controlador de barramento de cartão, enquanto PCIe não. A ROM 224 pode ser, por exemplo, um sistema de entrada/saída binário flash (BIOS). O acionador de disco rígido 226 e o CD-ROM 230 podem utilizar, por exemplo, um dispositivo eletrônico

integrado (IDE) ou um dispositivo de interface *Serial Advanced Technology Attachment* (SATA). Um dispositivo super I/O SIO) 236 pode ser acoplado a ponte sul e ao hub controlador de I/O 204.

[0066] Um sistema operacional é executado na unidade de processamento 206 e coordena e fornece o controle de vários componentes no sistema de processamento de dados 200 da Figura 2. O sistema operacional pode ser um sistema operacional disponível comercialmente, como o Microsoft ® Windows ® XP (Microsoft e Windows são marcas registradas da Microsoft Corporation nos Estados Unidos, outros países, ou ambos). Um sistema de programação orientada a objetos, tal como o sistema de programação Java ™, pode funcionar em conjunto com o sistema operacional e oferecer chamadas para o sistema operacional a partir de programas ou aplicações Java em execução no sistema de processamento de dados 200. Java e todas as marcas baseadas em Java são marcas registradas da Sun Microsystems, Inc. nos Estados Unidos, outros países, ou ambos.

[0067] Instruções para o sistema operacional, para o sistema de programação orientado a objetos, e aplicativos ou programas estão localizados em dispositivos de armazenamento, como o acionar de disco rígido 226, e podem ser carregados na memória principal 208 para execução pela unidade de processamento 206. Os processos das concretizações ilustrativas podem ser realizados pela unidade de processamento de 206 usando instruções implementadas por computador, que podem estar localizadas em uma memória, como, por exemplo, a memória principal 208, a memória só de leitura (ROM) 224, ou em um ou mais dispositivos periféricos.

[0068] O hardware das figuras 1-2 pode variar dependendo da implementação. Outros dispositivos de hardware interno ou periféricos, tais como a memória flash, memória equivalente não-volátil, ou unidades de disco óptico e similares, podem ser utilizadas em complemento ou em substituição aos equipamentos descritos nas figuras 1-2. Além disso, os processos de concretizações ilustrativas podem ser aplicados a um sistema de processamento de dados multiprocessador.

[0069] Em alguns exemplos ilustrativos, o sistema de processamento de dados 200 pode ser um assistente pessoal digital (PDA), que geralmente é configurado com memória flash para fornecer memória não-volátil para armazenar arquivos do sistema operacional e/ou de dados gerado pelo usuário. Um sistema de barramento pode ser composto de um ou mais barramentos, como um barramento de sistema, um barramento de I/O e um barramento PCI. Claro que o sistema de barramento pode ser implementado usando qualquer tipo de tecido de comunicações ou arquitetura que forneça uma transferência de dados entre os diferentes componentes ou dispositivos conectados ao tecido ou arquitetura. A unidade de comunicações pode incluir um ou mais dispositivos usados para transmitir e receber dados, como um modem ou um adaptador de rede. A memória pode ser, por exemplo, a memória principal 208 ou um cache tal como encontrado na ponte norte e no hub controlador de memória 202.

[0070] Uma unidade de processamento pode incluir um ou mais processadores ou CPUs. Os exemplos descritos nas figuras 1-2 e os exemplos descritos acima não são destinados a implicar limitações arquitetônicas.

[0071] Por exemplo, o sistema de processamento de dados 200 também pode ser um computador “tablete”, computador portátil, telefone ou outro dispositivo além de adotar a forma de um PDA.

[0072] O protocolo de controle de transmissão/ Protocolo da *Internet* (*Transmission Control Protocol*/*Internet Protocol* - TCP/IP) é um conjunto de protocolos de comunicação usados para conectar dispositivos de computação em uma rede, como na rede 102 da Figura 1. O *Transmission Control Protocol* e o *Internet Protocol* são os protocolos padrão para a transmissão de dados através de redes, tais como a *Internet*.

[0073] Passando agora a Figura 3, um modelo de referência básico de diagrama de blocos de uma interconexão de sistemas abertos (OSI) é mostrado de acordo com uma concretização ilustrativa. O modelo de referência

de interconexão 300 de sistemas abertos é um modelo comum de camadas de protocolo padrão para a definição de interoperabilidade e comunicação entre dispositivos de rede. Neste exemplo de sistemas abertos o modelo de referência de interconexão 300 inclui a transmissão de controle Protocolo de protocolo da *Internet* (Suite TCP/IP).

[0074] TCP/IP e protocolos semelhantes são utilizados por sistemas abertos em arquiteturas de comunicações de interconexão. Neste exemplo, a arquitetura inclui a camada de aplicação 302, a camada de apresentação 304, a camada de sessão 306, a camada de transporte 308, a camada de rede 310, a camada de link de dados 312 e a camada física 314. Cada camada é responsável pelo tratamento de várias funções e/ou tarefas de comunicação.

[0075] A camada de aplicação 302 lida com os detalhes do aplicativo específico que está sendo acessado e/ou executados. Muitas aplicações comuns TCP/IP estão presentes em quase toda a aplicação, incluindo uma Telnet para acesso remoto, um protocolo de transferência de arquivos (FTP), um protocolo de transferência de correio simples (SMTP) para o correio eletrônico, e um protocolo de gestão de rede simples (SNMP).

[0076] O software de aplicação tratado pela camada de aplicativo 302 pode incluir qualquer número de aplicações de software projetado para reagir aos dados através da porta de comunicações para fornecer a funcionalidade desejada que o usuário procura. As aplicações a esse nível podem incluir aquelas necessárias para lidar com dados, vídeo, gráficos, fotografias e/ou texto que possa ser acessado por usuários da *Internet*.

[0077] A camada de apresentação 304 inclui um protocolo de apresentação e um serviço de apresentação. O serviço de apresentação é usado para identificar uma sintaxe de transferência acertada que será utilizada. O protocolo de apresentação permite que usuários se comuniquem com o serviço de apresentação.

[0078] A camada de sessão 306 é composta de um protocolo de sessão e um serviço de sessão. O serviço de sessão fornece serviços para o usuário, incluindo, mas não se limitando a, estabelecer conexões entre usuários do serviço e da sessão, encerrando conexões entre os usuários, realizando negociações para o uso de ”tokens” de camada de sessão, e sincronizar pontos nos dados transmitidos para permitir que a sessão seja recuperada em caso de erro ou interrupção. O protocolo de sessão permite que usuários se comuniquem com o serviço de sessão.

[0079] Em seguida, a camada de transporte 308 fornece uma interface entre a camada de rede 310 e a camada de aplicação 302, que facilita a transferência de dados entre dois computadores anfitriões. A camada de transporte 308 se preocupa com coisas tais como, mas não se limitando a, dividir os dados passados para ela pela aplicação em pedaços de tamanho adequado para a camada de rede abaixo, acusando recebimento dos pacotes recebidos, e estabelecendo limites de tempo para garantir que o outro extremo acuse recebimento dos pacotes que são enviados. Na Suite do Protocolo TCP/IP, dois protocolos de transporte nitidamente diferentes estão presentes, o protocolo de controle de transmissão (TCP) e protocolo de datagrama do usuário(UDP).

[0080] O protocolo de controle de transmissão (*Transmission Control Protocol*) fornece serviços de confiabilidade para assegurar que os dados sejam devidamente transmitidos entre dois anfitriões, incluindo a detecção de abandono e serviços de retransmissão. Por outro lado, o protocolo de datagrama de usuário fornece um serviço muito mais simples para a camada de aplicação 302 pelo simples envio de pacotes de dados relativamente simples, chamados de datagramas de um anfitrião para outro. Datagramas são transmitidos sem que se forneça qualquer mecanismo para garantir que os dados no datagrama sejam devidamente transferidos. Quando o protocolo de datagrama de usuário for usado, a camada de aplicação 302 deve executar a funcionalidade de confiabilidade. Um exemplo de informações de pacotes dados da camada de transporte inclui, mas não está limitado a, um número de

porta para um anfitrião de origem e/ou um número de uma porta para um anfitrião de destino.

[0081] A camada de rede 310, que também pode ser referida como a camada de *Internet*, controla o movimento de pacotes de dados pela rede. Por exemplo, a camada de rede 310 lida com o encaminhamento de vários pacotes de dados que são transferidos através da rede. A camada de rede 310 na suíte TCP/IP é composta de vários protocolos, incluindo o protocolo de *Internet* (IP), o protocolo de mensagem de controle da *Internet* (ICMP), e o protocolo de gestão de grupo *Internet* (IGMP).

[0082] O Protocolo da *Internet* (IP) pode incluir, mas não está limitado a, o protocolo *Internet* versão 4 (IPv4), o protocolo da *Internet* versão 6 (IPv6), ou qualquer outra versão conhecida ou disponível de protocolo de *Internet*. Um exemplo de informações de pacotes de dados da camada da rede pode incluir, mas não estão limitadas a, um protocolo de *Internet* (IP) para identificar um endereço IP do anfitrião de origem e/ou um endereço IP do anfitrião de destino.

[0083] A amada de conexão 312 também pode ser referida como a camada de ligação ou a camada de interface de rede e normalmente inclui o acionador de dispositivo no sistema operacional e o correspondente cartão de interface de rede no computador. A camada de conexão 312 geralmente lida com todos os detalhes de hardware fisicamente interface com a camada física, 314, tais como, mas não se limitando a uma placa de interface de rede Ethernet e/ou um adaptador sem fio à *Internet*. Um exemplo de ligação de dados informações de pacotes da camada de dados podem incluir, mas não está limitado a um controle de acesso à mídia (MAC).

[0084] A camada física 314 refere-se aos meios de comunicação de rede a ser utilizados, tais como cabos ópticos ou cabos Ethernet. Em outras palavras, a camada física 314 é o cabo de rede física que conecta um dispositivo de computação, como o cliente 110 da Figura 1, a uma rede, como a rede 102 da Figura 1.

[0085] O mecanismo das concretizações ilustrativas pode ser mais especificamente implementado em uma camada, como a camada de transporte 308 e/ou a camada de rede 310.

[0086] A Figura 4 é um diagrama de blocos usado atualmente que ilustra um mecanismo de proteção de varredura de porta.

[0087] A rede de dados do sistema de processamento de 400 é um sistema de processamento de dados, incluindo dois ou mais dispositivos de computação conectados a uma rede, como o sistema de processamento de dados da rede 100 da Figura 1. Neste exemplo, a rede é a *Internet*. No entanto, a rede também pode incluir uma rede de área local, uma rede de área ampla, uma Ethernet, ou qualquer outro tipo de rede.

[0088] A rede de dados sistema de processamento de 400 inclui o anfitrião malicioso 402 e a vítima 404.

[0089] O anfitrião malicioso 402 é um hacker ou outro usuário não autorizado em um dispositivo de computação, como o cliente 110 da Figura 1, realizando uma varredura de portas da vítima 404. Em outras palavras, O anfitrião malicioso 402 está tentando localizar um ponto de acesso aberto vulnerável na vítima 404 de modo que o anfitrião malicioso 402 possa ganhar acesso não autorizado a vítima 404 e/ou lançar um ataque à vítima 404 através da porta aberta. O anfitrião malicioso 402 está realizando uma varredura de portas da vítima 404 para localizar pontos de acesso aberto vulneráveis para uso em um ataque contra a vítima 404.

[0090] A vítima 404 é um dispositivo de computação que hospeda um ou mais pedidos e/ou serviços. O anfitrião malicioso 402 está conectado a uma rede, como a rede 102 da Figura 1. Um dispositivo de computação cliente pode acessar os aplicativos e/ou serviços disponíveis na vítima 404, pedindo uma ligação a uma porta associada a uma determinada aplicação ou serviço através de uma conexão de rede.

[0091] A vítima 404 inclui a proteção de varredura de portas 405. A proteção de varredura de portas é qualquer software disponível para proteção de varredura de portas para detectar varreduras de portas e bloqueio de um endereço IP de origem do anfitrião malicioso 402. Um método comum através do qual a proteção de varredura de portas 405 funciona é através do acompanhamento de um conjunto de portas fechadas, que não estão sendo usados pela vítima 404, mas pode ser usada por hackers para fins de exploração devido a vulnerabilidades associadas com as aplicações associadas com as portas. A proteção de varredura de portas 405 pressupõe que usuários legítimos não iriam tentar acessar uma porta no conjunto de portas fechadas, pois os usuários legítimos saberiam que a vítima 404 não fornece aplicações ou serviços associados no conjunto de portas fechadas. Apenas anfitriões maliciosos, como o anfitrião malicioso 402, tentam se conectar a uma porta do conjunto de portas fechadas, porque eles estão pescando (em busca) de serviços vulneráveis escutando nas portas.

[0092] Se a proteção de varredura de portas 405 detecta um pacote de dados pedindo uma conexão para um porta do conjunto de portas fechadas, tal como um pacote de dados de sincronização (SYN) ou um padrão desses pacotes de dados provenientes de um determinado anfitrião remoto, a proteção de varredura de portas 405 vai evitar ou bloquear todo o tráfego do anfitrião remoto específico. Desta forma, mesmo se o anfitrião remoto tiver detectado uma porta vulnerável aberta, o anfitrião remoto não será capaz de lançar um ataque, porque todo o tráfego futuro rede do anfitrião remoto está bloqueada.

[0093] Neste exemplo, o anfitrião malicioso 402 realiza uma varredura de portas, enviando uma série de pacotes de dados a vítima 404 solicitando uma conexão para uma ou mais portas bem conhecidas da vítima 404. O pacote de dado 406 é um da série de pacotes de dados enviados pelo O anfitrião malicioso 402.

[0094] O pacote de dados 406 é um pacote de dados de protocolo de controle de transmissão / protocolo *Internet* (TCP/IP) contendo uma solicitação para se conectar a uma porta identificada como porta "n" da vítima 404. Neste

exemplo, o pacote de dados 406 é a mensagem de sincronização do protocolo de controle de transmissão (TCP SYN) que pede a conexão para a porta "n". A porta “n" pode ser qualquer número de porta, como a porta 80 associada ao tráfego do protocolo de transferência de hipertexto.

[0095] Neste exemplo, o pacote de dados 406 inclui um endereço IP de origem fake ou falso. Um endereço de origem IP é um endereço IP que identifica o remetente de um pacote de dados. Um endereço IP de falsa origem é um endereço IP que identifica uma vítima incidental 408 em vez do remetente real de pacotes de dados 406. A vítima incidental 408 pode ser um dispositivo de computação real ou a vítima incidental 408 pode não existir realmente. Em outras palavras, o falso endereço IP utilizado pelo anfitrião malicioso 402, não tem que identificar um dispositivo de computação real. Neste exemplo, o pacote de dados 406 inclui o endereço IP de origem "A" associado à vítima incidental 408 em vez de endereço IP "B", que é o real endereço IP do anfitrião malicioso 402.

[0096] Em resposta ao recebimento do pacote de dados 406, a vítima 404 envia o pacote de dados 410 para a vítima incidental 408. O pacote de dados 410 é um protocolo de controle de transmissão/Protocolo da *Internet* de pacotes de dados que indica se a porta "X" é uma porta aberta ou uma porta fechada. Neste exemplo, o pacote de dados 410 é mensagem de acusar recebimento (do pedido) de sincronizar (SYN/ACK). O pacotes de dados 410 está sendo enviado para um endereço IP de destino "A" associado a vítima incidental 408. Portanto, o anfitrião malicioso 402 não receberá o pacote de dados 410 no decurso da transmissão da mensagem da vítima 404 para a vítima incidental 408.

[0097] Por não ser o anfitrião malicioso 402 o destinatário dos pacotes de dados 410, o anfitrião malicioso 402 espiona 412 os pacotes de dados 410 da rede. Espionar refere-se a capturar ou a espiar um pacote de dados que se destinava a ser enviado para um dispositivo de computação de diferente destino. Neste exemplo, o anfitrião malicioso 402 utiliza um farejador para espionar o pacote de dados 410 destinado e a ser recebido pela vítima

incidental 408. Um farejador de pacotes é uma aplicação que captura pacotes de dados transmitidos através da rede apesar do fato do anfitrião malicioso não ser o destinatário do pacote de dados.

[0098] Assim, o anfitrião malicioso 402 é informado quanto à porta "X" ser uma porta aberta que pode ser vulnerável a ataques. Se a porta "X" é uma porta aberta, o anfitrião malicioso 402 lança um ataque 414 contra a vítima 404.

[0099] A vítima 404 tem software atual de proteção de varredura de porta. A versão atual de proteção de varredura de porta permite às vítimas 404 reconhecer os pacotes de dados 406 como uma possível varredura de porta de um hacker, tal como o anfitrião 402. A versão atual de proteção de varredura de portas permite a vítima 404 bloquear mensagens subsequentes do endereço IP de origem identificada em uma varredura de porta suspeita, tal como o pacote de dados 406. No entanto, como o endereço IP de origem no pacote de dados 406 é um endereço IP falso, a vítima 404 não vai conseguir bloquear mensagens do anfitrião malicioso 402, tais como mensagens do anfitrião malicioso 402 associadas ao ataque 414. Desta forma, o anfitrião malicioso 402 pode ser capaz de ignorar o atual software de proteção de varredura para atacar e, eventualmente, desativar ou comprometer a vítima 404.

[00100] Assim, neste exemplo, o anfitrião malicioso 402 é um varredor de porta que está tentando se conectar a uma porta vulnerável, enviando um pacote TCP SYN, tal como o pacote de dados 406, para uma determinada porta da vítima 404. O pacote de dados 406 gerado pelo anfitrião malicioso 402 inclui um endereço de IP falso para uma vítima incidental que pode ou não existir. Se não houver um programa ou aplicativo escutando uma dada porta, a vítima 404 responde enviando um TCP SYN/ACK, tal como um pacote de dados 410 para a vítima incidental.

[00101] O anfitrião malicioso 402 monitora a rede e vê passar os pacotes de dados 410. O anfitrião malicioso 402 determina que determinada porta é uma porta aberta que pode ser conectada para exploração de qualquer vulnerabilidade existente no aplicativo associado com a porta. O anfitrião

malicioso 402 pode determinar qual aplicativo está associado com a porta de dados com base nos números de porta bem conhecidos atribuídos a cada porta.

[00102] A proteção de varredura de portas 405 da vítima 404 responde ao pacote falso, bloqueando o endereço IP de origem falso "A" para a vítima incidental 408. O anfitrião malicioso 402 está livre para enviar ataque 414 à determinada porta da vítima 404 usando a ferramenta de *hacking* apropriada para este porta particular e o programa de aplicação vulnerável associado a porta particular.

[00103] As concretizações ilustrativas reconhecem que quando o software de proteção de varredura de portas atual responde a um pacote de dados falsos usando um endereço IP de origem falsificado recebido de um hacker, durante uma varredura de portas, o software de proteção de varredura de portas responde, bloqueando o falso endereço IP de origem da vítima incidental, em vez do endereço IP real para o anfitrião verdadeiro mal-intencionado. O software de proteção de varredura de portas atual falha quanto a identificar e bloquear o verdadeiro endereço IP da origem de onde endereços IP de origem falsos são fornecidos por um anfitrião malicioso. Portanto, as concretizações ilustrativas reconhecem a necessidade de um software de proteção de varredura de portas reforçado que evite um endereço IP que na verdade lançando um ataque tão rapidamente quanto possível depois de uma varredura de portas ser detectada.

[00104] Assim, as concretizações ilustrativa fornecem um método implementado por computador, um aparelho e um programa de computador de código utilizável por computador para proteção varredura de portas. Em uma modalidade, o processo gera um pacote de dados de resposta com um cabeçalho modificado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta em resposta à detecção de uma varredura de portas.

[00105] Nas concretizações ilustrativas descritas abaixo, o cabeçalho modificado para o protocolo que é utilizado para transmitir pacotes de dados é um cabeçalho de protocolo de controle de transmissão. No entanto, as

concretizações ilustrativas não se limitam a modificar cabeçalhos de protocolos de controle de transmissão. As concretizações ilustrativas podem modificar um cabeçalho em qualquer tipo de protocolo conhecido ou disponível utilizado para a transmissão de pacotes de dados sobre uma conexão de rede para formar uma resposta modificada do pacote de dados, incluindo, mas não se limitando a, o protocolo de controle de transmissão ou o protocolo de datagrama de utilizador (UDP).

[00106] O pacote de dados modificado de resposta irá obter uma resposta de um destinatário do pacote de dados modificado. O processo envia o pacote de dados de resposta a um primeiro endereço de encaminhamento associado à varredura de portas. O processo identifica um segundo endereço de encaminhamento em um cabeçalho do pacote de dados de resposta em resposta ao recebimento de uma resposta ao pacote de dados de resposta modificado. Nos exemplos descritos abaixo, o primeiro endereço de encaminhamento é um primeiro endereço de protocolo de *Internet* e o segundo o endereço de encaminhamento é um segundo endereço de protocolo de *Internet*. O protocolo de *Internet* pode ser qualquer versão do protocolo de *Internet*, incluindo, mas não limitado a, protocolo *Internet* versão 4 (IPv4), protocolo *Internet* versão 6 (IPv6), ou qualquer outra versão do protocolo *Internet*. Além disso, as concretizações ilustrativas não se limitam ao Protocolo *Internet*. Qualquer tipo de protocolo conhecido ou disponível para a prestação de roteamento de endereços para um ou mais portas podem ser utilizado de acordo com as concretizações ilustrativas.

[00107] O segundo endereço de encaminhamento é um endereço de encaminhamento real de uma origem de varredura de portas. Todo o tráfego de rede do segundo endereço de encaminhamento pode ser bloqueado para prevenir um ataque a quaisquer portas abertas.

[00108] Passando agora à Figura 5, um diagrama de blocos que ilustra um fluxo através de um sistema de proteção de varredura de portas para a detecção de uma varredura de portas com um falso endereço IP de origem é mostrado de acordo com uma modalidade ilustrativa. O computador 500 pode

ser implementado usando qualquer tipo de dispositivo de computação, incluindo mas não limitado a, o servidor de 106 ou os clientes 110 da Figura 1.

[00109] O computador 500 inclui o conjunto de aplicativos ou aplicações 502. O conjunto de aplicações 502 é um conjunto de uma ou mais aplicações e/ou serviços disponíveis no computador 500. Um aplicativo é um software de computador que usa os recursos de um dispositivo de computação para executar uma tarefa ou serviço para um usuário.

[00110] O conjunto de aplicações de 502 pode ser armazenado em um dispositivo de armazenamento de dados, como dispositivo de armazenamento de dados 504. O dispositivo de armazenamento de dados 504 é qualquer tipo conhecido ou disponível de dispositivo para armazenamento de dados, incluindo, mas não limitados a, memória principal, um banco de dados, uma memória somente leitura (ROM), uma memória de acesso aleatório (RAM), uma memória não-volátil de acesso aleatório (NV-RAM), um disco rígido, uma memória flash, um disquete, um disco compacto regravável (CD-RW), ou qualquer outro tipo de dispositivo de armazenamento de dados. Neste exemplo, dispositivo de armazenamento de dados 504 está localizado no computador 500. No entanto, o dispositivo de armazenamento dados 504 também pode estar localizado remotamente em relação ao computador 500.

[00111] Computador 500 utiliza o protocolo de controle de transmissão / protocolo *Internet* (TCP / IP) 506 para transmitir e receber mensagens de outros dispositivos de computador conectados a uma rede, como a rede de 102 da Figura 1. O TCP/IP 506 é um conjunto de protocolos padrão para fornecer uma conexão entre um transmissor e um destinatário. O TCP/IP 506 pode fornecer entregas garantidas e assegurar que os pacotes são recebidos em uma sequência correta. Em outras palavras, quando as mensagens são enviadas de outro dispositivo de computador para o computador 500, as mensagens podem não ser recebidos em ordem. Portanto, o TCP/IP 506 utiliza os números de sequência do protocolo de controle de transmissão (TCP) para garantir que as mensagens sejam entregues a camada de aplicativos na ordem correta.

[00112] O TCP/IP 506 dá um número de sequência para cada mensagem que é enviada pelo TCP/IP 506 para que um destinatário das mensagens possa determinar a ordem correta das mensagens. Números de sequência inicial (ISN s) são trocados entre o computador de 500 e um segundo dispositivo de computação quando a conexão entre o computador de 500 e o segundo dispositivo de computação é estabelecida. O TCP/IP 506 permite a recepção de mensagens com números de sequência que estão fora da sequência , se os números fora-de-sequência estiverem dentro de certos limites ou limitações. No entanto, se o número de sequência estiver muito fora da faixa esperada de sequência de números, a mensagem será desconsiderada ou identificada como uma mensagem ruim. Em tais casos, o computador 500 pode solicitar ao segundo computador reenviar a mensagem com o número de sequência ruim.

[00113] O TCP/IP 506 inclui as portas 508 e 510. Neste exemplo, o computador 500 é descrito como tendo duas portas. No entanto, o computador 500 pode ter qualquer número de portas.

[00114] A porta 508 tem um número de porta atribuído e é associada a uma aplicação do conjunto de aplicações 502. Por exemplo, se a porta 508 estiver associada com a um aplicativo para tratar do tráfego do protocolo de transferência de hipertexto, então a porta 508 teria atribuído a ela o número da porta 80. Neste exemplo, a porta 508 é uma porta aberta.

[00115] A porta 510 também tem um número de porta atribuído. Neste exemplo, a porta 510 tem o número de porta 20 atribuído para protocolo de transferência de arquivos (FTP). No entanto, neste exemplo, o protocolo de transferência de arquivos não está disponível no computador 500. Portanto, a porta 510 é uma porta fechada.

[00116] O computador 500 também inclui a proteção de varredura de portas reforçada 512. A proteção de varredura de portas reforçada 512 é o software de proteção de varreduras de portas para detectar e bloquear endereços IP associados a um anfitrião malicioso ou outro dispositivo de computação que exerça a varredura de portas, como o anfitrião malicioso 516.

[00117] O anfitrião malicioso 516 é um hacker, cracker, ou usuário não autorizado, ou usuário ilegítimo a executar uma varredura de portas em uma ou mais portas associadas ao computador 500, tais como as portas 508 e 510.

[00118] O anfitrião malicioso 516 inclui a suíte TCP/IP 518 de protocolos para envio e recebimento de pacotes de dados através da rede. O anfitrião malicioso 516 se conecta ao computador 500 por essa conexão de rede.

[00119] O anfitrião malicioso 516 inclui o varredor de portas 520. O varredor de portas 520 pode ser qualquer tipo de dispositivo conhecido ou disponível para a realização de uma varredura de portas de um conjunto de uma ou mais portas no computador 500. O varredor de portas 520 pode ser implementado inteiramente por software ou como uma combinação de hardware e software. Neste exemplo, o varredor de portas 520 gera o pacote de dados de varredura de porta 522. O pacote de dados de varredura de porta 522 inclui o falso endereço de origem IP 524. O falso endereço de origem IP 524 não é um endereço IP associado ao anfitrião malicioso 516. O falso endereço de origem IP 524 pode ser um endereço IP para um dispositivo de computação real, diferente do anfitrião malicioso 516, ou o falso endereço de origem IP 524 pode ser um endereço IP para um dispositivo de computação que realmente não existe.

[00120] A varredura de portas de proteção reforçada 512 inclui a detecção de endereços de origem IP 514. A detecção de endereços de origem IP 514 é um componente de software para geração de pacote de dados de resposta 526. O pacote de dados de resposta 526 é um pacote de dados que é modificado para obrigar o TCP/IP 518 do anfitrião malicioso 516 a gerar a resposta 528. Em outras palavras, se a varredura de portas de proteção reforçada 512 detectar uma varredura de portas, a varredura de portas de proteção reforçada 512 responde enviando pacotes de dados de resposta 526 para anfitrião malicioso 516 que fará com que o anfitrião malicioso 516 envie a resposta 528. A resposta 528 pode incluir uma sinalização de redefinir (reset) (RST) ou de acusação de término (FIN/ACK) no cabeçalho do protocolo de controle de transmissão da resposta 528.

[00121] Neste exemplo, a resposta 528 também inclui o real endereço IP do anfitrião malicioso 530 na camada de rede do cabeçalho do protocolo de controle de transmissão de resposta 528.

[00122] O computador 500 pode identificar o endereço IP real do anfitrião malicioso 530 da resposta 528.

[00123] A varredura de portas de proteção reforçada 512, em seguida, evita ou bloqueia o endereço IP real 530 do anfitrião malicioso 516 para evitar futuros ataques do anfitrião malicioso 516.

[00124] Em seguida, a Figura 6 é um diagrama de blocos ilustrando um mecanismo de proteção de varredura de portas de acordo com uma concretização ilustrativa. O sistema de processamento de dados de rede 600 é um sistema de processamento de dados que inclui vários dispositivos de computação conectados através de uma rede, tais como o sistema de processamento de dados da rede 100 da Figura 1. Neste exemplo, a rede é a *Internet*. No entanto, a rede também pode incluir uma rede de área local, uma rede de área ampla, uma Ethernet, ou qualquer outro tipo de rede. O sistema de processamento de dados da rede 600 inclui o anfitrião malicioso 602 e a vítima 604.

[00125] O anfitrião malicioso 602 é um hacker ou outro usuário não autorizado em um dispositivo de computação, como o cliente 110 da Figura 1, ou o anfitrião malicioso 516 da Figura 5. O anfitrião malicioso 602 está realizando uma varredura de portas não autorizada na vítima 604 na tentativa de localizar um ponto de acesso vulnerável aberto para que o anfitrião malicioso 602 possa ganhar acesso não autorizado a vítima 604 e/ou lançar um ataque à vítima 604 através da porta aberta.

[00126] A vítima 604 é um dispositivo de computação que hospeda um ou mais aplicativos e/ou serviços, tais como o servidor 106 na Figura 1 ou o computador 500 da Figura 5. Um dispositivo de computação cliente pode acessar os aplicativos e/ou serviços disponíveis na vítima 604 pedindo uma conexão a uma porta associada a um determinado aplicativo ou serviço através de uma conexão de rede.

[00127] A vítima 604 inclui a proteção reforçada de varredura de portas 605 que por sua vez inclui o software de detecção de endereço IP de origem, tal como a proteção reforçada de varredura de portas 512 da Figura 5. A proteção reforçada de varredura de portas 605 é um software para utilização na identificação de um endereço IP do anfitrião malicioso 602 quando o anfitrião malicioso 602 lançar uma varredura de portas através do envio do pacote de 606 usando um falso endereço IP de origem e bloquear o endereço IP do anfitrião malicioso 602 em vez de bloquear o falso endereço IP de origem usado pelo anfitrião malicioso 602.

[00128] O anfitrião malicioso 602 realiza uma varredura de portas, enviando uma série de pacotes de dados para a vítima 604 solicitando uma conexão com uma ou mais portas bem conhecidas da vítima 604. O pacote de dados 606 é um de uma série de pacotes de dados enviados pelo anfitrião malicioso 602 para uma porta da vítima 604, tal como o pacote de dados de varreduras de portas 522 da Figura 5.

[00129] O pacote de dados por 606 é um pacote de dados de protocolo de controle de transmissão/Protocolo da *Internet* solicitando uma conexão a uma porta identificada como porta "n" da vítima 604. Neste exemplo, o pacote de dados 606 é um pacote de dados de protocolo de controle de transmissão de sincronização (TCP SYN). A porta “n" pode ser qualquer número de porta, como a porta 80 associada ao tráfego de *Hypertext Transfer Protocol*.

[00130] O pacote de dados por 606 inclui um endereço de origem IP fake ou falso para uma vítima incidental. A vítima incidental pode ou não existir de fato. Neste exemplo, o pacote de dados 606 inclui o endereço IP de origem "A" associado a uma vítima incidental, em vez de endereço IP "B", que é o real endereço IP do anfitrião malicioso 602.

[00131] Em resposta ao recebimento do pacote de dados 606, gera pacotes de dados 608. O pacote de dados 608 é uma pacote de dados de resposta, como o pacote de resposta dados 526 da Figura 5. O pacote de dados 608 é produzido de forma que o pacote de dados obterá uma resposta do anfitrião malicioso 602 se o anfitrião malicioso 602 espionar o pacote de dados 608 de fora da rede. O cabeçalho do protocolo de controle de

transmissão (TCP) de pacotes de dados 608 é alterado de uma forma que vai enganar a camada TCP/IP do anfitrião malicioso e levá-la a responder ao pacote de dados 608 se o anfitrião malicioso 602 espionar o pacote de dados 608 da rede.

[00132] Por exemplo, se a porta reforçada de varredura de portas 605 oferecer um número de sequência ruim a camada TCP/IP DO anfitrião malicioso 602 vai responder através do envio de uma sinalização de sincronização (SYN), na tentativa de se reconectar à vítima 604. Um número de sequência ruim é um número de sequência que está fora do intervalo esperado ou aceitável de números de sequência possíveis.

[00133] Uma sinalização de finalização (FIN) indica o fim de uma sessão. Quando um pacote de dados, incluindo uma sinalização de finalização, é recebido, o TCP/IP envia automaticamente um aviso de recebimento de finalização em resposta. Assim, se a proteção de varredura de portas 605 der ao pacote de dados 608 a sinalização de finalização, a camada de TCP/IP do anfitrião malicioso 602 irá enviar automaticamente uma sinalização de reconhecimento de finalização (FIN/ACK) em uma mensagem de resposta à vítima 604.

[00134] Assim, neste exemplo, a proteção reforçada de varreduras de porta 605 envia o pacote de dados 608 para a vítima incidental associada ao falso endereço IP de origem. O pacote de dados 608 é um protocolo de controle de transmissão/Protocolo da *Internet* de pacotes de dados que indica se n "porta" é uma porta aberta ou uma porta fechada. Neste exemplo, o pacotes de dados 608 contém uma sinalização de reconhecimento (SYN/ACK) e um número de sequência ruim. A vítima 604 envia o pacote de dados 608 para o falso endereço IP "A" associado à vítima incidental.

[00135] A camada de conexão de dados no cabeçalho do pacote de dados 608 indica um endereço de controle de acesso à mídia (MAC) para o destino do pacote de dados 608. O endereço de controle de acesso à mídia especifica o adaptador de rede particular do dispositivo de computação de destino. Neste caso, o endereço de controle de acesso à mídia especifica o adaptador de rede da vítima incidental.

[00136] Normalmente, se anfitrião malicioso 602 não estivesse funcionando no modo de espionagem, o anfitrião malicioso 602 não receberia o pacotes de dados 608, porque o endereço controle de acesso à mídia da camada de conexão de dados não coincidiria com o adaptador de rede associado ao anfitrião malicioso 602. No entanto, neste exemplo, o anfitrião malicioso 602 está em modo de espionagem. Assim, o controlador Ethernet associado ao anfitrião malicioso 602 irá ignorar o endereço controle de acesso à mídia do cabeçalho do pacote de dados 608 e passará o pacote de dados 608 até a camada de protocolo TCP/IP associado ao anfitrião malicioso 602.

[00137] O anfitrião malicioso 602 espiona os pacotes de dados 608 da rede. Neste exemplo, o anfitrião malicioso 602 utiliza um “farejador” para espionar o pacote de dados 608 da rede. Em resposta a detecção de um número de sequência ruim no pacote de dados 608, a camada de TCP/IP do anfitrião malicioso 602 automaticamente gera e transmite um pacote de dados de resposta 610 para a vítima 604 em uma tentativa de reconectar-se a vítima 604. O pacote de dados 610 é um pacote de dados de resposta, tal como a resposta 528 da Figura 5.

[00138] O pacote de dado 610 contém o real endereço IP de origem "B" do anfitrião malicioso 602 em vez do falso endereço IP "A". A proteção reforçada de varredura de portas 605 bloqueia o endereço IP de origem "B" de para parar o envio de outras mensagens para a vítima 604 da rede. Desta forma, anfitrião malicioso 602 é impedido de lançar qualquer ataque em quaisquer portas vulneráveis da vítima 604.

[00139] A Figura 7 é uma ilustração exemplar de pacotes de varredura de portas transmitidos durante uma varredura de portas de acordo com a concretização ilustrativa. O pacote de varredura de portas 702 é um pacote de dados com um falso endereço IP de origem gerado por um anfitrião malicioso, tais como o pacote de dados de varredura de portas 522 da Figura 5 e/ou o pacote de dados 606 da Figura 6. Neste exemplo, a varredura de portas é um pacote de dados de sincronização (SYN).

[00140] O pacote de dados de resposta 703 é um pacote de dados gerado por um destinatário do pacote de varredura de portas 702, tal como o pacote de

dados de resposta 526 da Figura 5 e/ou o pacote de dados 608 da Figura 6. O destinatário é uma vítima do anfitrião malicioso. O pacote de dados de resposta 703 é gerado pela vítima e enviado para o endereço IP falso. Neste exemplo, a resposta é um pacote de dados para acusar reconhecimento de sincronização (SYN/ACK) gerado por uma vítima do anfitrião malicioso, como a vítima 604 da Figura 6.

[00141] O pacote de varredura de portas 702 inclui informações para a camada de conexão de dados na seção 704. A via de transmissão do pacote de dados de varredura de portas do anfitrião host malicioso à vítima pretendida irá atribuir a Ethernet (ETH) o endereço de controle de acesso à mídia (MAC) com base em tabelas de encaminhamento/roteamento.

[00142] O pacote de dados de varredura de portas 702 também inclui informações na camada de rede. A informação da camada de rede inclui um falso endereço IP de origem "A" na linha 705. O falso endereço IP de origem "A" é um endereço IP para uma vítima incidental existente ou inexistente, e não o real endereço IP do anfitrião malicioso que gerou o pacote de dados de varredura de portas 702. A informação da camada de rede no pacote de dados inclui também um endereço IP de destino 706 para identificar o dispositivo de computação da vítima.

[00143] A informação da camada de transporte no pacote de dados de varredura de portas 702 identifica um número de porta de origem para o hacker mal-intencionado e um número de porta de destino para o dispositivo de computação anfitrião da vítima, como mostrado na linha 708. A linha 710 é um número de sequência para o pacote de varredura de portas. A linha 712 identifica o pacote de dados como um pacote de dados de sincronização (SYN) solicitando uma conexão com o dispositivo de computação da vítima.

[00144] O pacote de dados de resposta 703 inclui um endereço IP de origem da vítima 714 e endereço IP de destino 716. O endereço IP de destino 716 é o falso endereço IP usado pelo hacker mal intencionado.

[00145] A informação da camada de transporte inclui um número de porta de origem para o dispositivo de computação da vítima gerando o pacote de dados de resposta, como mostrado na linha 714. A linha 716 inclui um

endereço IP de destino. O endereço IP de destino, neste exemplo é o falso endereço IP da vítima incidental. A vítima incidental pode ou não existir de fato.

[00146] A linha 722 pode fornecer um número de sequência ruim. O número de sequência ruim é um número de sequência que está fora do intervalo esperado ou aceitável de números de sequência possíveis.

[00147] A linha 722 indica que o pacote de resposta de dados 703 é um pacote de dados de acusação de reconhecimento/sincronização (SYN / ACK). Em outro exemplo, a linha 722 poderia indicar que o pacote de resposta de dados 703 é um pacote de dados de redefinir (RST) ou de terminar (FIN).

[00148] Em outras palavras, usando o software de proteção de varredura de portas disponível, se a vítima tinha um serviço ativo na porta 23, que pode ser identificado na linha 708, a vítima iria responder gerando um pacote de dados de resposta de acusação de reconhecimento/sincronização (SYN/ ACK). Este seria o final da sessão, entre a porta 23 da vítima e a porta 1494 do anfitrião malicioso. O anfitrião malicioso, então, saberia que a vítima tinha um serviço de telnet rodando na porta 23. O anfitrião mal intencionado poderia então lançar um ataque telnet na porta 23. O software de proteção de varredura de portas atual bloquearia o falso endereço IP identificado na linha 705 do Pacote de varredura de portas, mas seria incapaz de bloquear o endereço IP real do anfitrião malicioso. Assim, o anfitrião malicioso estaria livre para atacar a porta 23.

[00149] Em conformidade com as concretizações de exemplo, quando a vítima recebe um pacote de varredura de varredura de portas 702, o software de proteção de varredura de porta da vítima reage de tal forma a obrigar o anfitrião real malicioso a responder. Por exemplo, o software de proteção reforçada de varredura de porta gera um pacote de resposta 703, que inclui um número de sequência ruim, uma mensagem de redefinir (RST), ou uma mensagem de encerramento/finalização (FIN). Dado que o anfitrião incidental nunca enviou um pacote de varredura de varredura de portas 702, o anfitrião incidental não irá responder ao pacote de dados de resposta 703. Em vez disso, se o anfitrião incidental realmente existe, o anfitrião incidental apenas ignorará o pacote de dados de resposta 703. Se o anfitrião não existe, então o

anfitrião hospedeiro incidental não pode responder ao pacote de dados de resposta 703. Assim, apenas do anfitrião é esperado que responda ao pacote de dados de resposta 703. Desta forma, a vítima pode identificar e bloquear o endereço IP real de um anfitrião malicioso que usa uma varredura de portas para identificar as portas abertas que possam ser vulneráveis a ataques pelo anfitrião malicioso.

[00150] Referindo-se agora a Figura 8, um fluxograma ilustrando um processo para a detecção de uma varredura de portas com um endereço IP falso é retratado de acordo com uma concretização ilustrativa. Neste exemplo ilustrativo mostrado na Figura 8, o processo é realizado por um componente de software proteção de varredura de portas, tal como a proteção de varredura de portas 512 da Figura 5.

[00151] O processo começa por fazer uma determinação de uma varredura de portas estar sendo detectada (etapa 802). Se uma varredura de portas não for detectada, o processo retorna para a etapa 802 até que uma varredura de portas seja detectada. A varredura de portas pode ser detectada quando um pacote de dados de varredura de portas ou uma série de pacotes de dados for recebido de um anfitrião malicioso.

[00152] Se uma varredura de portas for detectada na etapa 802, o processo gera um pacote de dados de resposta modificado (etapa 804). O processo envia o pacote de dados de resposta modificado para o endereço IP de origem identificado no pacote de dados de varredura de portas (etapa 806). Neste exemplo, o endereço IP de origem é um falso endereço IP de origem que não é um endereço IP correto do anfitrião realizando a varredura de portas.

[00153] O processo então faz uma determinação de uma resposta para a resposta ter sido recebida (etapa 808). Se a resposta não tiver sido recebida, o processo retorna para a etapa 808 até que uma resposta seja recebida. Quando uma resposta é recebida na etapa 808, o processo bloqueia todo o tráfego de rede de um segundo endereço IP identificado no cabeçalho do protocolo de controle de transmissão da resposta (etapa 810) para impedir quaisquer ataques que possam ser lançados a partir da varredura de portas de origem com o processo se encerrando em seguida.

[00154] A Figura 9 é um fluxograma ilustrando um processo para modificar uma resposta de pacotes de dados, de acordo com uma concretização ilustrativa. Neste exemplo da Figura 9, o processo pode ser implementado por um componente de software para proteção de varredura de portas, tal como a proteção de varredura de portas reforçada 512 da Figura 5.

[00155] O processo começa com a geração de um pacote de dados de resposta (etapa 902). O processo faz uma determinação quanto a modificar o pacote de dados de resposta pela adição de um número de sequência ruim para o cabeçalho do protocolo de controle de transmissão para o pacote de dados de resposta (etapa 904). Se a determinação for feita para modificar o pacote de dado de resposta pela adição de um número de sequência ruim, o processo adiciona um número de sequência ruim para o cabeçalho do pacote de dados de resposta (etapa 906) e transmite o pacote de dados de resposta para a vítima incidental (etapa 908) com o processo se encerrando em seguida.

[00156] Voltando a etapa 904, se for feita uma determinação quanto a uma sequência de números ruins não ser adicionada, o processo faz uma determinação quanto a adicionar um sinalizador de redefinir ou de finalização ao pacote de dados de resposta (etapa 910). Se o processo determinar que a sinalização não será adicionada o processo termina em seguida.

[00157] Voltando a etapa 910, se o processo faz a determinação de modificar o pacote de dados de resposta adicionando um sinalizador de redefinir ou finalização, o processo adiciona um sinalizador de redefinir ou um de finalização (etapa 912) ao pacote de dados de resposta. O processo, em seguida, envia o pacote de dados de resposta modificado à vítima incidental (etapa 908) com o processo se encerrando em seguida.

[00158] Assim, as concretizações ilustrativas fornecem um método implementado por computador, aparelho e programa de computador de código utilizável por computador para a proteção de varredura de portas. Em uma concretização, o processo gera um pacote de dados de resposta com um cabeçalho de protocolo de controle de transmissão modificado para formar um pacote de dados de resposta modificado em resposta à detecção de uma varredura de portas. O pacote de dados de resposta irá obter uma resposta de

um destinatário do pacote de dados modificado. O processo envia o pacote de dados de resposta a um primeiro endereço protocolo de *Internet* associado a varredura de portas.

[00159] O processo identifica um segundo endereço de protocolo de *Internet* em um cabeçalho do pacote de dados de resposta em resposta ao recebimento de uma resposta ao pacote de dados de resposta modificado. O segundo endereço de protocolo de *Internet* é um endereço de protocolo de *Internet* real de uma origem de varredura de porta. Todo tráfego de rede do segundo endereço de protocolo de *Interne*, pode então ser bloqueado para prevenir um ataque a quaisquer portas abertas.

[00160] O cabeçalho modificado do protocolo de controle de transmissão pode incluir um número de sequência ruim. Um número de sequência ruim é um número de sequência que não se enquadra em uma faixa aceitável de números de sequência. Em outra concretização, o cabeçalho modificado do protocolo de controle de transmissão pela transmissão do cabeçalho do protocolo de controle pode incluir um sinalizador de redefinir ou de finalização. Em outra concretização, o protocolo de controle pela transmissão é gerado pela alteração de uma quantidade usada para gerar o pacote de dados de resposta modificado.

[00161] Desta forma, os ataques contra portas abertas e potencialmente vulnerável por hackers que usam endereços IP falsos pode ser evitado.

[00162] O fluxograma e diagramas de blocos nas figuras ilustram a arquitetura, funcionalidade e operação de possíveis implementações de sistemas, métodos e produtos de programa de computador, de acordo com várias concretizações. Neste sentido, cada etapa do fluxograma ou bloco de diagramas pode representar um módulo, segmento ou porção de código, que compreende uma ou mais instruções executáveis para implementar a função lógica especificada. É também de salientar que, em algumas implementações alternativas, as funções indicadas nas etapas podem ocorrer fora da ordem anotada nas figuras. Por exemplo, duas etapas mostradas em sucessão podem, de fato, ser executadas substancialmente simultaneamente, ou as

etapas podem, às vezes, ser executadas na ordem inversa, dependendo da funcionalidade envolvida.

[00163] A invenção pode assumir a forma de uma concretização totalmente de hardware, uma modalidade totalmente de software ou uma personalizada contendo tanto elementos de hardware quanto de software. Em uma concretização preferida, a invenção é implementada por software, o qual inclui, porém não está limitado a, firmware, software residente, microcódigo, etc.

[00164] Além disso, a invenção pode assumir a forma de um produto de programa de computador acessível a partir de um meio utilizável por computador ou um meio legível por computador que forneça código de programa para uso por ou em conexão com um computador ou qualquer outro sistema de execução de instrução.

[00165] Para os efeitos desta descrição, um meio legível utilizável por computador pode ser qualquer aparelho tangível, que possa conter, armazenar, comunicar, propagar, ou transportar o programa para uso por, ou em conexão com, o sistema, aparelho ou dispositivo de execução da instrução,

[00166] O meio pode ser um registro eletrônico, magnético, óptico, eletromagnético, infravermelho, ou um sistema de semicondutores (ou aparelho ou dispositivo), ou um meio de propagação. Exemplos de um meio legível por computador inclui uma fita de semicondutores ou memória de estado sólido, magnético, um disquete de computador removível, uma memória de acesso aleatório (RAM), uma memória somente leitura (ROM), um disco magnético rígido e um disco óptico. Exemplos atuais de discos ópticos incluem disco compacto - *Read Only Memory* (CD-ROM), disco compacto - leitura/gravação (CD-R / W) e DVD.

[00167] Um sistema de processamento de dados adequado para a armazenagem e/ou execução de código de programa vai incluir, no mínimo, um processador acoplado, direta ou indiretamente, a elementos da memória através de um barramento do sistema.

[00168] Os elementos de memória podem incluir memória local contratada durante a execução efetiva do código do programa, o armazenamento em

massa, e memórias cache que fornecem armazenamento temporário de, pelo menos, algum programa de cooperação a fim de reduzir o número de vezes que o código deve ser recuperado do armazenamento em massa durante a execução.

[00169] Dispositivos de entrada/saída (ou I/O devices) incluindo, mas não se limitando aos teclados, monitores, dispositivos apontadores, etc., podem ser acoplados ao sistema, quer diretamente quer através de controladores de E/S intervenientes.

[00170] Os adaptadores de rede também podem ser acoplados ao sistema para permitir que o sistema de processamento de dados torne-se associado a outros dados ou sistemas de processamento de impressoras remotas ou dispositivos de armazenamento através de redes intervenientes privadas ou públicas. Modems, cable modem e placas Ethernet são apenas alguns dos tipos disponíveis atualmente de adaptadores de rede.

[00171] A descrição da presente invenção foi apresentada para fins de ilustração e descrição, e não pretende ser exaustiva ou limitada à invenção na forma divulgada. Muitas modificações e variações serão aparentes para aqueles com competências normais na técnica. A concretização foi escolhida e descrita, a fim de melhor explicar os princípios da invenção, a aplicação prática, e para permitir a outros com competências normais na técnica compreender a invenção de várias modalidades, com várias alterações que podem ser adequadas ao uso específico contemplado.

REIVINDICAÇÕES

1. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, caracterizado pelas etapas de:

em resposta a detecção de uma varredura de porta, gerar, através de um processador, um pacote de dados de resposta com um cabeçalho modificado para se adequar a um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta modificado, onde o pacote de dados de resposta modificado obtenha uma resposta de um destinatário do pacote de dados de resposta modificado, onde o cabeçalho modificado obrigue a camada de protocolo da internet/protocolo de controle de transmissão do destinatário a responder ao pacote de dados de resposta modificado em resposta ao destinatário que espionar o pacote de dados de resposta modificado;

enviar o pacote de dados de resposta modificado para um endereço de protocolo da internet de uma primeira fonte associada a varredura de porta; e

em resposta ao recebimento do pacote de dados de resposta modificado, identificar se um endereço de protocolo da internet de uma segunda fonte em um cabeçalho da resposta é um endereço de protocolo da internet de uma fonte correta de uma fonte de varredura de porta, onde o endereço de protocolo da internet da segunda fonte seja diferente do endereço de protocolo da internet da primeira fonte.

2. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo incluir um número de sequência que está fora de uma faixa aceitável de números de sequência.

3. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 2, caracterizado por:

o número de sequência fora de uma faixa aceitável de números de sequência ser uma violação do protocolo que irá provocar uma resposta do destinatário.

4. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 2, caracterizado por:

o número de sequência fora de uma faixa aceitável de números de sequência ser um número de sequência que está fora de um intervalo de números de sequência aceitável.

5. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo inclui um sinalizador de redefinir.

6. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

onde o cabeçalho modificado para se adequar ao protocolo incluir um sinalizador de chegada.

7. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

modificar o cabeçalho incluir ainda alterar uma quantidade usada para gerar o pacote de dados de resposta modificado.

8. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

bloquear todo o tráfego de rede proveniente do segundo endereço de encaminhamento para evitar um ataque a quaisquer portas abertas.

9. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

o primeiro endereço de encaminhamento primeiro não ser um endereço de encaminhamento correto de um dispositivo de computação.

10. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

em resposta ao recebimento de um pacote de dados de varredura de portas, identificar um endereço de encaminhamento de origem em um cabeçalho do pacote de dados de varredura de portas como o primeiro endereço de encaminhamento.

11. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo ser um cabeçalho do protocolo de controle de transmissão.

12. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo ser um cabeçalho de protocolo de datagrama do usuário modificado.

13. MÉTODO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM, de acordo com a reivindicação 1, caracterizado por:

uma camada de link de dados no cabeçalho modificado indicar um endereço de controle de acesso de meios para um destino do pacote de dados de resposta modificado.

14. APARELHO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM caracterizado por:

um sistema de barramento;

um sistema de comunicação conectado ao sistema de barramento;

uma memória conectada ao sistema de barramento

onde a memória inclui com um código de programa de computador de utilizável por computador; e

uma unidade de processamento conectados ao sistema de barramento, onde a unidade de processamento executa o código de programa utilizável por computador para

gerar um pacote de dados de resposta com um cabeçalho modificado para se adequar a um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta modificado em resposta à detecção de uma varredura de porta, onde o pacote de dados de resposta modificado obtém um pacotes de dados de resposta de um destinatário do pacote de dados de resposta modificado, onde o cabeçalho de dados modificado obriga a camada de protocolo da internet/protocolo de controle de transmissão do destinatário a responder ao pacote de dados de resposta modificado em resposta ao destinatário que espionar o pacote de dados de resposta modificado;

enviar o pacote de dados de resposta modificado para um endereço de protocolo da internet de uma primeira origem associada a varredura de porta; e

identificar se um endereço de protocolo da internet de uma segunda origem em um cabeçalho do pacote de dados de resposta em resposta ao recebimento do pacote de dados de resposta é um endereço de protocolo da internet de uma origem correta de uma varredura de porta, onde o endereço de protocolo da internet da segunda fonte seja diferente do endereço de protocolo da internet da primeira fonte.

15. APARELHO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo incluir um número de sequência que está fora de uma faixa aceitável de números de sequência.

16. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 15, caracterizado por:

o número de sequência fora de uma faixa aceitável de números de sequência ser uma violação do protocolo que irá provocar uma resposta do destinatário do pacote de dados de resposta.

17. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo inclui um sinalizador de redefinir.

18. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

o cabeçalho modificado para se adequar ao protocolo inclui um sinalizador de chegada.

19. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

a unidade de processamento executar o código de programa utilizável por computador para bloquear todo o tráfego de rede proveniente do segundo endereço de encaminhamento para evitar um ataque a quaisquer portas abertas.

20. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

o cabeçalho modificado adequado ao protocolo ser um cabeçalho de protocolo de controle de transmissão modificado.

21. APARELHO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 14, caracterizado por:

uma camada de link de dados no cabeçalho modificado indicar um endereço de controle de acesso de meios para um destino do pacote de dados de resposta modificado.

22. EQUIPAMENTO PARA DETECÇÃO DE VARREDURRAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM caracterizado por:

compreender um computador anfitrião, onde o computador anfitrião inclui

um software de proteção de varredura de portas reforçado para

detectar pacotes de dados de varredura de portas e

gerar um pacote de dados de resposta com um cabeçalho adequado para um protocolo utilizado para transmitir pacotes de dados para formar um pacote de dados de resposta em resposta à detecção de uma varredura de portas, onde o pacote de dados de resposta modificado obtém um pacote de dados de resposta de um destinatário do pacote de dados de resposta modificado, onde o cabeçalho modificado obriga a camada de protocolo da internet/protocolo de controle de transmissão do destinatário a responder ao destinatário que espionar o pacote de dados de resposta modificado, onde o pacote de dados de resposta modificado é enviado para um endereço de protocolo da internet de uma primeira origem associada a varredura de portas; e um detector de endereço de protocolo da internet de origem, onde o detector de endereço de protocolo da internet da origem identifica que um endereço de protocolo da internet de uma segunda origem em um cabeçalho de uma reposta a um pacote de dados de resposta modificado é o endereço de protocolo da internet da origem correta de uma origem da varredura de portas, onde o

endereço de protocolo da internet da segunda origem é diferente do primeiro endereço de protocolo da internet da primeira origem.

23. EQUIPAMENTO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 22, caracterizado por:

o cabeçalho modificado adequado ao protocolo incluir uma violação de protocolo que desencadeia a resposta de um destinatário do pacote de dados de resposta.

24. EQUIPAMENTO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 22, caracterizado por:

o cabeçalho modificado adequado para o protocolo incluir um sinalizador de redefinir ou um sinalizador de chegada.

25. EQUIPAMENTO PARA DETECÇÃO DE VARREDURAS DE PORTA COM FALSO ENDEREÇO DE ORIGEM de acordo com a reivindicação 22, caracterizado por:

o computador anfitrião ser um primeiro computador e ainda compreender um segundo computador que inclui

um varredor de portas, onde o varredor de portas executa a varredura de portas no primeiro computador enviando o pacote de dados de varredura contendo um endereço de encaminhamento de origem falsa para o primeiro computador,

o endereço de encaminhamento de origem falsa não é um endereço de encaminhamento correto para o segundo computador, e

uma camada de protocolo da internet/protocolo de controle de transmissão onde o protocolo da internet/protocolo de controle de transmissão gera automaticamente a resposta ao pacote de dados de resposta modificado.

FIG. 1

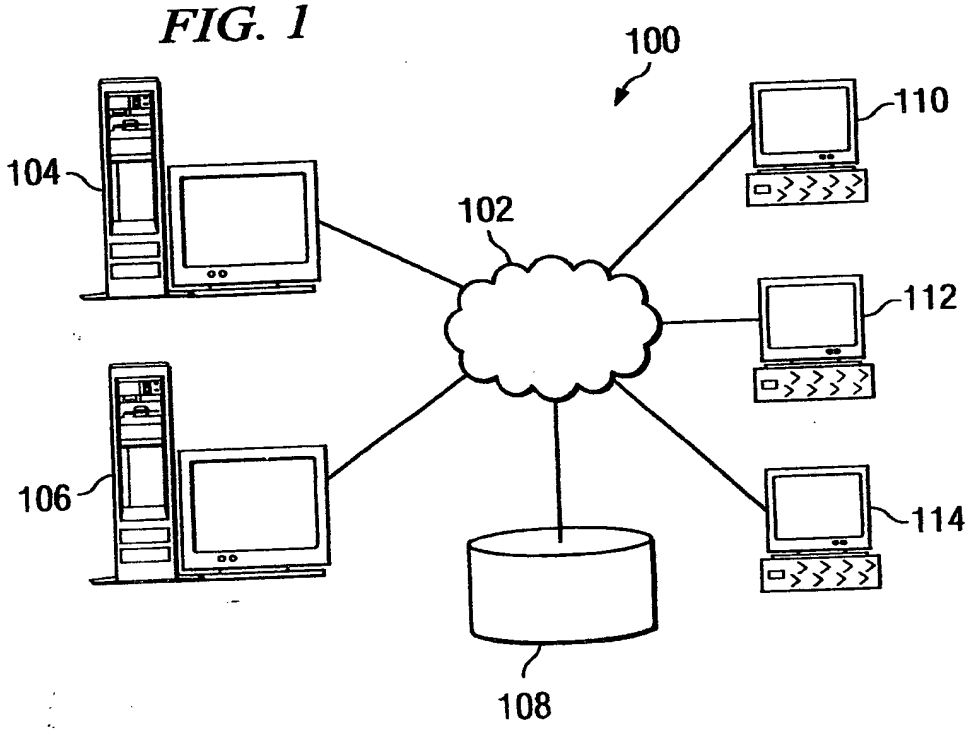
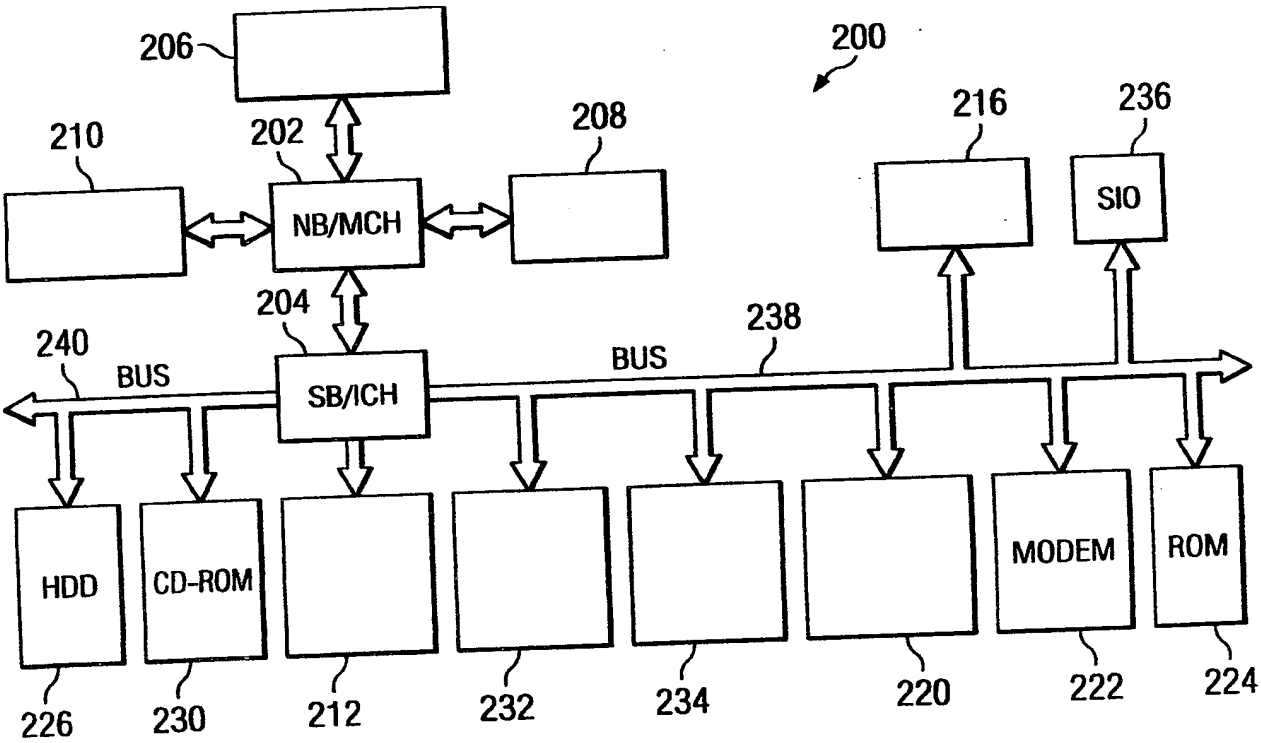

100
110
104
102
112
106
114
108

FIG. 2


206
200
216
236
210
202
208
SIO
NB/MCH
204
238
240
BUS
BUS
SB/ICH
HDD
CD-ROM
MODEM
ROM
226
230
212
232
234
220
222
224

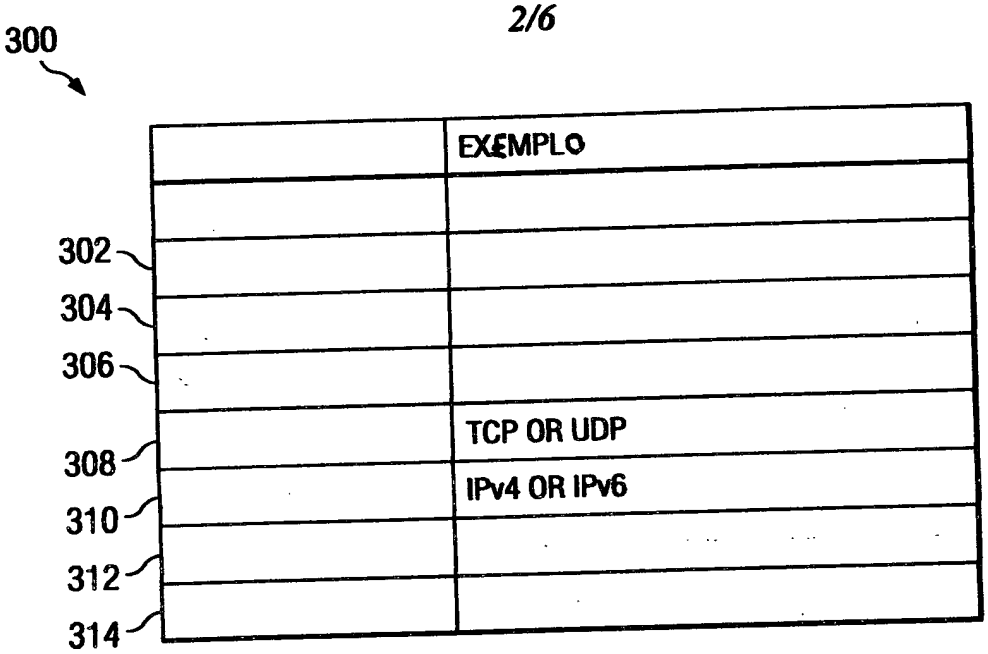

300
EXEMPLO
302
304
306
TCP OR UDP
308
IPv4 OR IPv6
310
312
314

FIG. 3

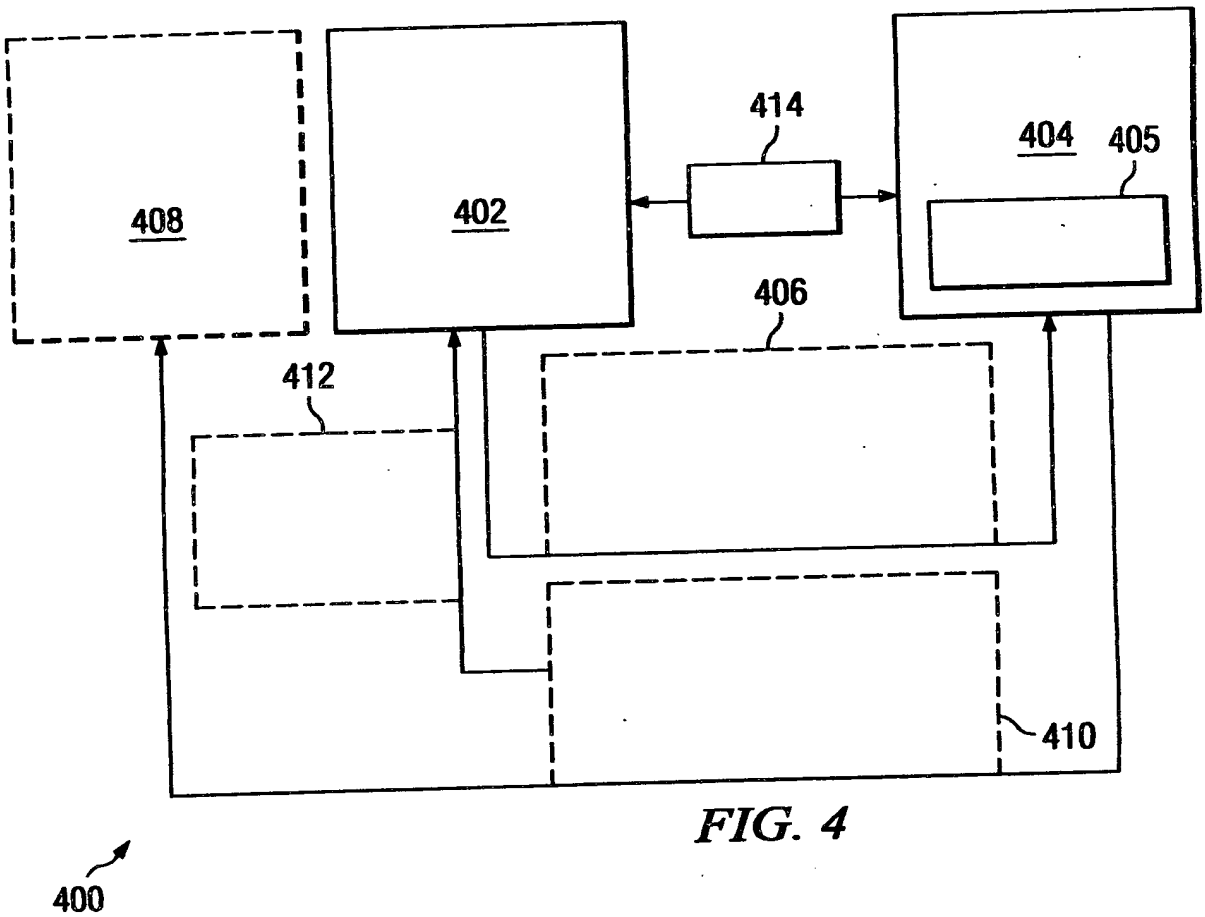

408
402
414
404
405
406
412
410
400

FIG. 4

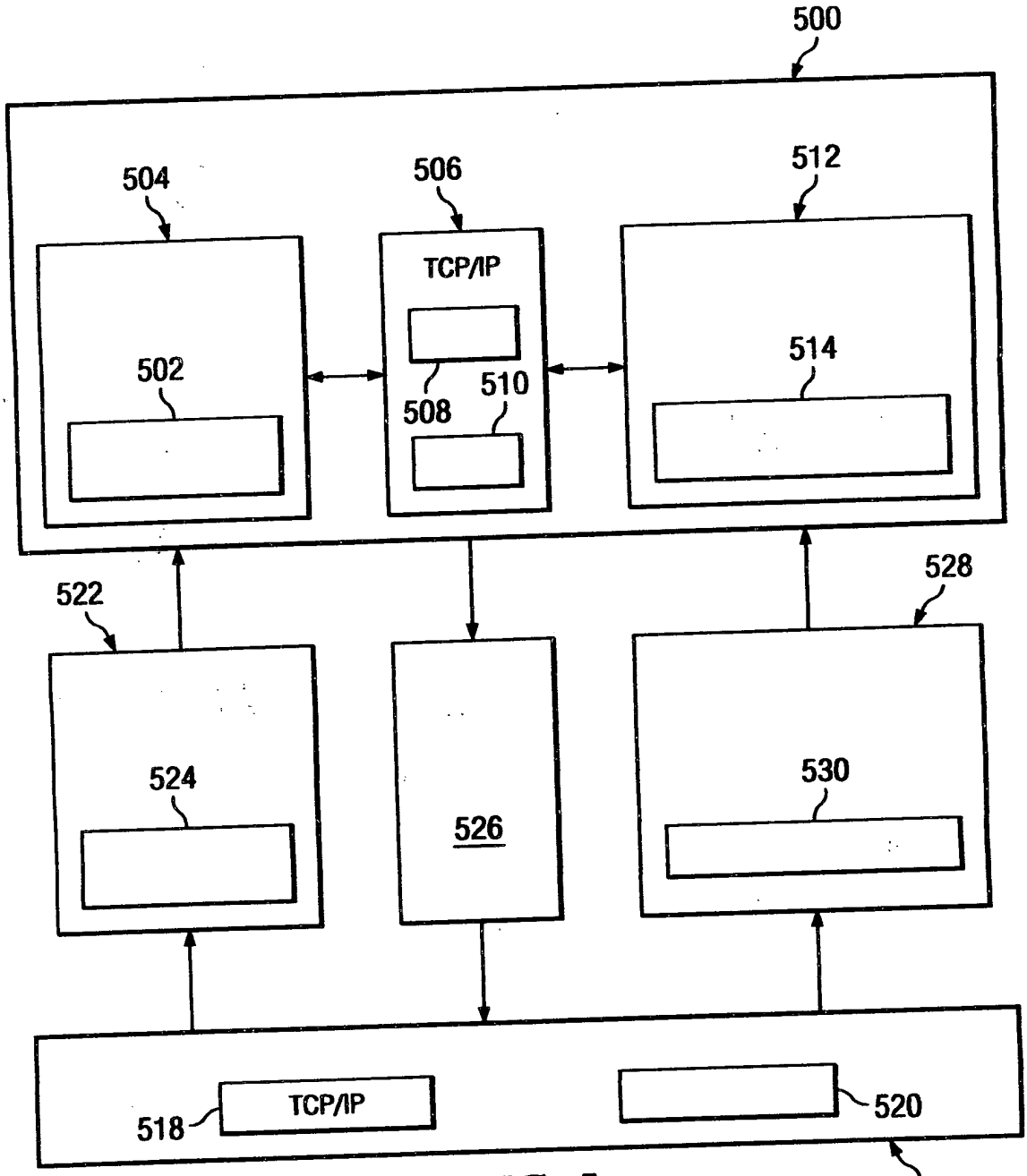

500
504
506
512
TCP/IP
502
508
510
514
522
528
524
526
530
518
TCP/IP
520
516

FIG. 5

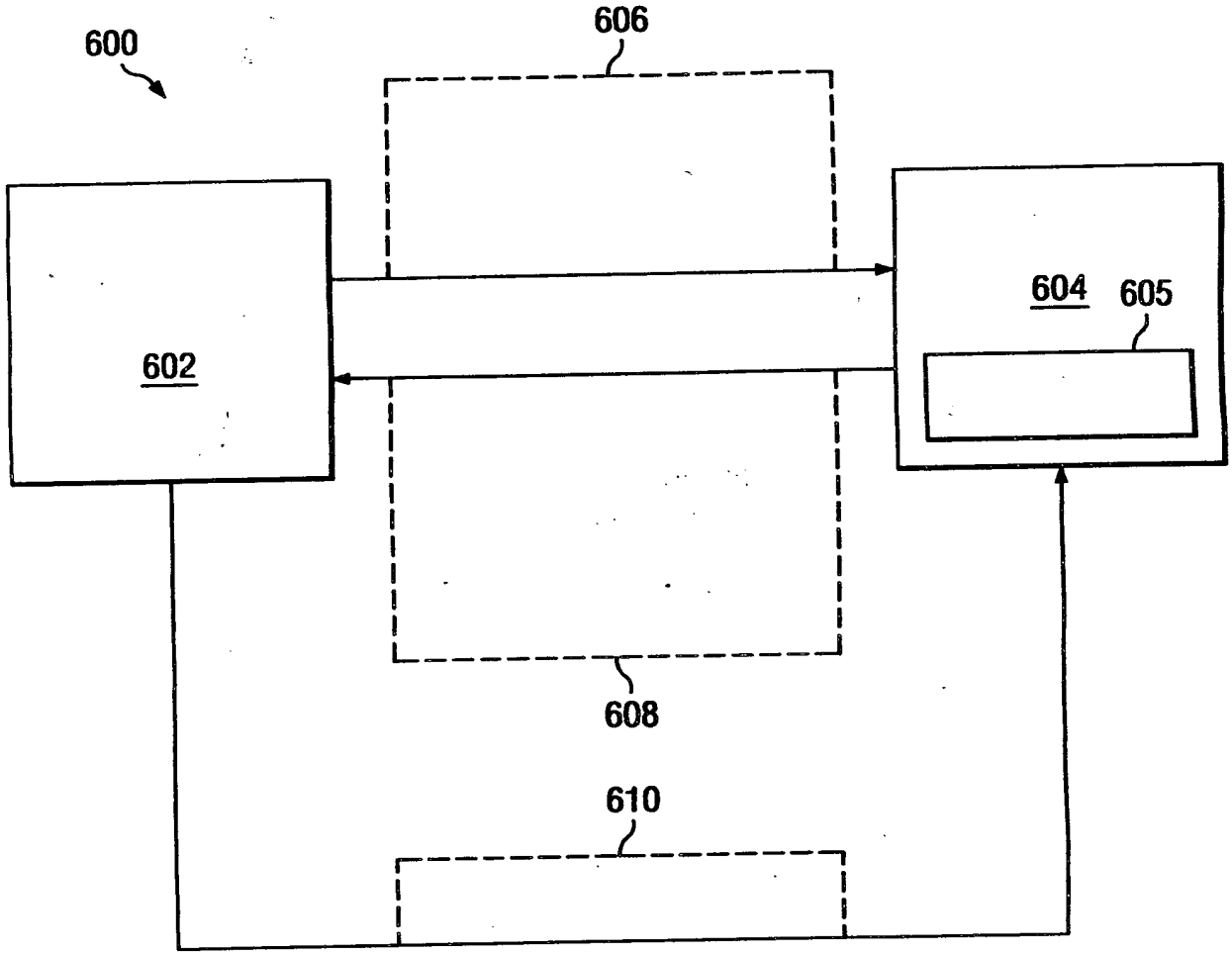


FIG. 6

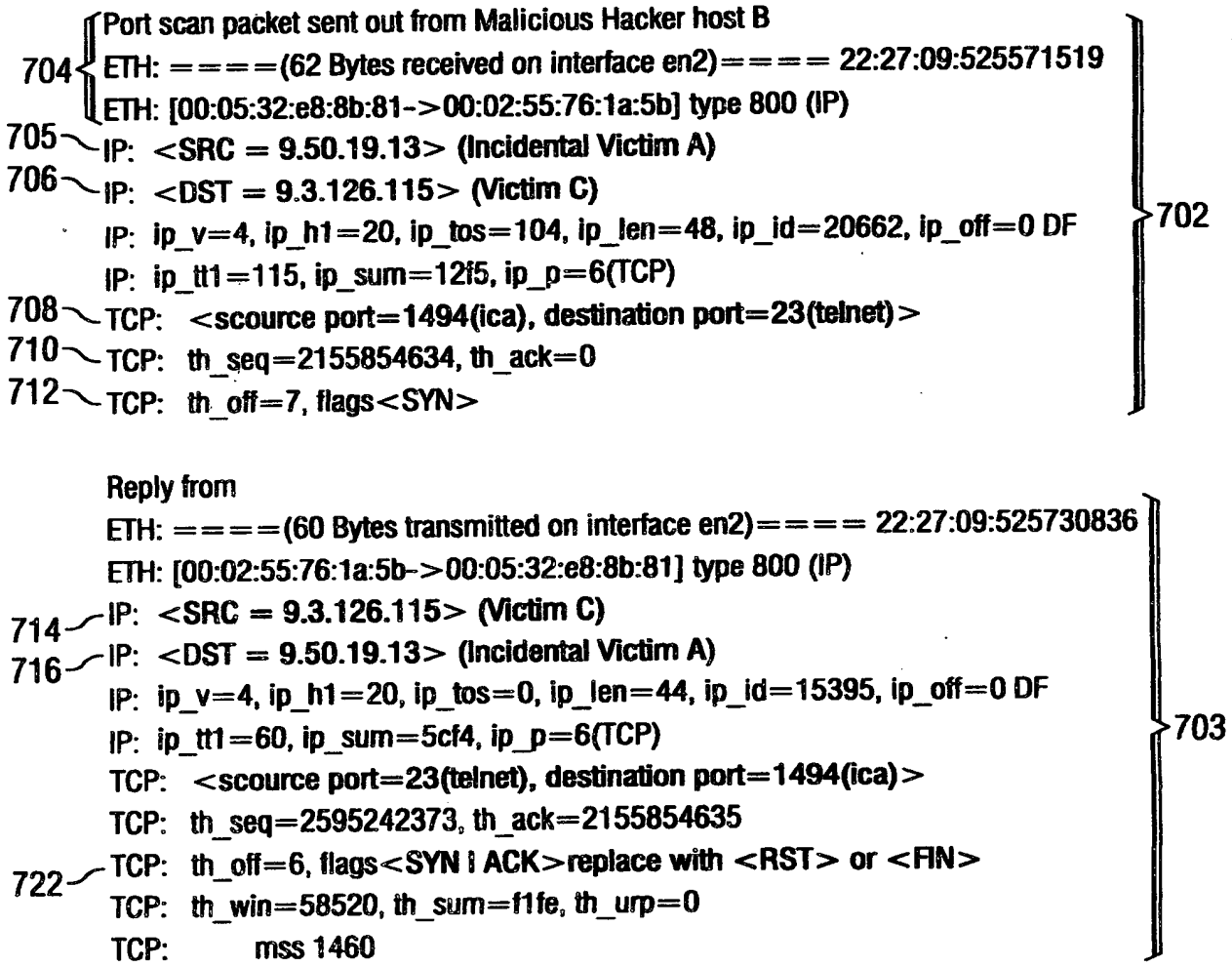

Port scan packet sent out from Malicious Hacker host B
704
ETH: =====(62 Bytes received on interface en2)===== 22:27:09:525571519
ETH: [00:05:32:e8:8b:81->00:02:55:76:1a:5b] type 800 (IP)
705
IP: <SRC = 9.50.19.13> (Incidental Victim A)
706
IP: <DST = 9.3.126.115> (Victim C)
IP: ip_v=4, ip_hl=20, ip_tos=104, ip_len=48, ip_id=20662, ip_off=0 DF
IP: ip_ttl=115, ip_sum=12f5, ip_p=6(TCP)
708
TCP: <scource port=1494(ica), destination port=23(telnet)>
710
TCP: th_seq=2155854634, th_ack=0
712
TCP: th_off=7, flags<SYN>
702
Reply from
ETH: =====(60 Bytes transmitted on interface en2)===== 22:27:09:525730836
ETH: [00:02:55:76:1a:5b->00:05:32:e8:8b:81] type 800 (IP)
714
IP: <SRC = 9.3.126.115> (Victim C)
716
IP: <DST = 9.50.19.13> (Incidental Victim A)
IP: ip_v=4, ip_hl=20, ip_tos=0, ip_len=44, ip_id=15395, ip_off=0 DF
IP: ip_ttl=60, ip_sum=5cf4, ip_p=6(TCP)
TCP: <scource port=23(telnet), destination port=1494(ica)>
TCP: th_seq=2595242373, th_ack=2155854635
722
TCP: th_off=6, flags<SYN | ACK>replace with <RST> or <FIN>
TCP: th_win=58520, th_sum=f1fe, th_urp=0
TCP: mss 1460
703

FIG. 7

FIG. 8

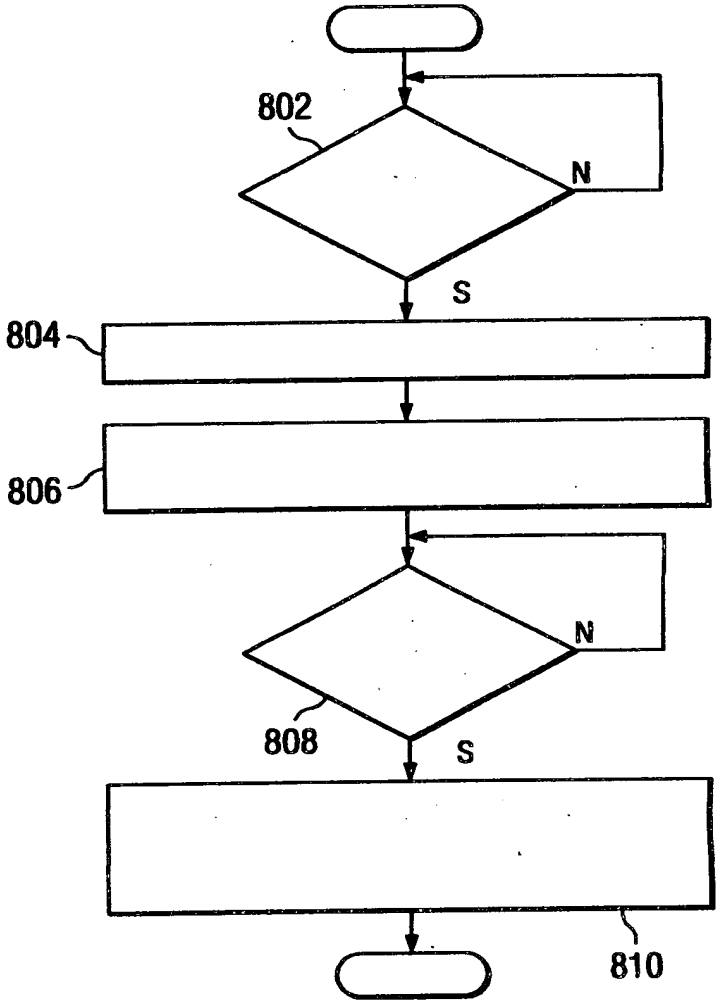


FIG. 9