Parte II

Vulnerabilidades,
Ameaças,
Riscos

Vulnerabilidades, Ameaças e Riscos

Capítulo 2: **Pensando em Ameaças e Riscos**

Capítulo 3: **Preparação para Ataques: Footprint** e **Fingerprint**

Capítulo 2

Pensando em Ameaças e Riscos

Objetivos

- Avaliar ameaças e riscos à segurança de redes.
- Após concluir este capítulo, você estará preparado para executar as seguintes tarefas:

Tarefas

- Identificar as necessidades de segurança de rede.
- Identificar algumas das causas dos problemas de segurança de rede.
- Identificar características e fatores motivadores de invasão de rede.

Tarefas

- Identificar as ameaças mais significativas na segurança de rede.
- Conceituar vulnerabilidade, ameaça, risco e gerenciamento de risco.

Por que segurança ... ?

- Porque para garantir a segurança nos negócios é preciso atualizar constantemente as defesas para reduzir a vulnerabilidade às ameaças inovadoras dos invasores.

Desafios

- **Segurança** é difícil de ser implementada uniformemente em toda a empresa.
- Escolha de uma alternativa ou combinação adequada de diversas opções de soluções.

Desafios

- Escolher entre várias opções diferentes e disponíveis e adotar aquelas que satisfaçam os requisitos exclusivos da rede e dos negócios.

Desafios

- Os produtos diferentes devem ser integrados em toda a empresa a fim de se atingir uma única política de segurança estável.

Porque temos problemas de segurança

- Fragilidade da Tecnologia
- Fragilidade de Configuração
- Fragilidade da Política de Segurança

Fragilidade da Tecnologia

- TCP/IP
- Sistema Operacional
- Equipamentos de Rede

Fragilidade de Configuração

- São problemas causados pelo fato de **não se configurar equipamentos interligados** para impedir problemas de segurança conhecidos ou prováveis.

Fragilidade de Configuração

- Considerações *default* inseguras nos produtos.
- Equipamento de rede configurado equivocadamente.
- Contas de usuários inseguras.
- Contas de sistemas com senhas previsíveis.

Fragilidade do Equipamento de Rede

- Proteção de senha insegura
- Falhas de autenticação
- Protocolos de Roteamento
- Brechas no Firewall

Fragilidades da Política de Segurança

- Falta de uma política escrita.
- Políticas internas
- Falta de continuidade dos negócios
- Controles de acesso para equipamentos de rede não são aplicados.
- A administração de segurança é negligente, inclusive a monitoração e a auditoria.

Fragilidades da Política de Segurança

- Falta de conhecimento sobre ataques.
- Alterações e instalação de software e hardware não seguem a política.
- Falta de Planejamento de Contingência.

Conheça seus invasores

- **Script Kiddie**

  Não possuem muita habilidade.

  Mas teve a sorte de encontrar um sistema remoto que não aplicou o *patch* de correção a tempo.

Script Kiddie

- Sãos bons na razão inversamente proporcional à negligência de administradores/usuários que não acompanham listas de segurança e demais páginas de fornecedores ou CERT (Computer Emergency Response Team)

Script Kiddie

- Um invasor que faz intrusão vinculada a uma falha conhecida.
- Não buscam informações e/ou máquinas específicas. Ou seja, ganhar acesso de root.
- Basta ter acesso para desconfigurar home pages de forma mais fácil possível.

Script Kiddie

- Sua técnica consiste em ficar revirando a Internet atrás de máquinas vulneráveis e fazer explorações com *exploits,* ferramentas que permitam explorar as falhas em serviços.

Script Kiddie

- Podem desenvolver suas próprias ferramentas.
- Existem os que não conhecem nenhuma técnica, e tudo o que sabem é executar as ferramentas fornecidas por outro script kiddie.

Cracker

- Um invasor de bons conhecimentos técnicos e assim sendo, ele será capaz de apagar seus rastros de maneira mais sutil.

- Se caracteriza pelo alto nível técnico, na medida em que cada passo da invasão é realmente estudado e bem pensado.

Cracker

- Busca dados como configurações padrões ou senhas padrões que ele possa explorar.
- Tem capacidade para desenvolve seus próprios *exploits*. São geniais e criativos para a má intenção.
- Realiza ataques inteligentes para comprometer a segurança da rede.

Cracker

- Suas atitudes furtivas poderão enganar até aos mais experientes administradores.
- São os verdadeiros invasores (intrusos) ou até mesmo criminosos cibernéticos.

Hacker

- Um programador apaixonado.
  Constroem e tornam o mundo melhor.

  Exemplos:

  Stallman, Linus Torvalds, Ada Lovelace, Douglas Engelbart, Dennis Ritchie, Ken Thompson, Arnaldo Melo, Marcelo Tossati, Alan Cox, ...

  Não são fúteis desconfiguradores de páginas.

Hacker

- (Hacking ou Hacking Ético)

  Programador ou administrador que se reserva a questionar os problemas de segurança nas tecnologias disponíveis e as formas de provar o conceito do que é discutido.

Hacker Ético

- Uma pessoa que investiga a integridade e a segurança de uma rede ou sistema operacional.
- Usa o conhecimento avançado sobre SW e HW para entrar no sistema através de formas inovadoras.

Hacker Ético

- Compartilha seu conhecimento gratuitamente através da Internet.
- Não usa de más intenções. Tenta oferecer um serviço à comunidade interessada.

Conceito de Invasor

- Script Kiddie
- Cracker
- Hacker
- Phracker (pessoas que fazem acesso não autorizado a **recursos de telecomunicações**)

Características de um Invasor

- Sabem codificar em várias linguagens de programação.
- Conhecimentos aprofundados sobre ferramentas, serviços e protocolos.
- Grande experiência com Internet.
- Conhecem intimamente pelo menos dois Sos.

Características de um Invasor

- Têm um tipo de trabalho que usa redes. Usam equipamentos como se fossem modo de vida.
- Colecionam SW e HW.
- Têm vários computadores para trabalhar.

Motivos para ameaças

- Exploração de emoções (Notoriedade, Diversão).
- Concorrência de mercado
- Inimigos políticos
- Ladrões (atividades furtivas)
- Espiões (Espionagem industrial)

Motivos para ameaças

- Funcionários hostis:

  empregados ou antigos empregados, vingança, ataque de Troca de Senhas ou Sessões Abertas)

- Investigação legal.

Vulnerabilidades

- Ausência de proteção cobrindo uma ou mais ameaças.
- Fraquezas no sistema de proteção.
- **Vulnerabilidades são claramente associadas com ameaças.**

Exemplos

- A **ameaça a acesso não autorizado** está ligada a **controles de acesso inadequados**.

- A **ameaça de perda de dados críticos** e apoio ao processamento se deve ao **planejamento de contingência ineficaz**.

Exemplo

- A **ameaça de incêndio** está associada a vulnerabilidade da **prevenção contra incêndio inadequada**.

Bens

- **Bens Tangíveis**

  Aqueles que são paupáveis: HW, SW, suprimentos, documentações, ...

- **Bens Intangíveis**

  Pessoa, reputação, motivação, moral, boa vontade, oportunidade, ...

Bens

- Os bens mais importantes são as **informações**.
- **Informações** ficam em algum lugar entre os bens tangíveis e os intangíveis.

Informações Sensíveis

- **Informações**, que se **perdidas**, mal usadas, acessadas por pessoas **não autorizadas**, ou **modificadas**, podem prejudicar uma organização, quanto ao funcionamento de um negócio ou a privacidade de pessoas.

O que é uma **ameaça** ?

- Uma **ameaça** é algum fato **que pode ocorrer e acarretar algum perigo** a um bem.
- Tal fato, se ocorrer, será causador de perda.
- É a **tentativa de um ataque**.

Agente de uma ameaça

- É uma entidade que pode iniciar a ocorrência de uma ameaça.

- Entidade: uma pessoa:

  invasor / intruso

Ameaças Não-Intencionais

- Erros humanos,
- Falhas em equipamentos,
- Desastres naturais,
- Problemas em comunicações.

Ameaças Intencionais

- Furto de informação,
- Vandalismo,
- Utilização de recursos, violando as medidas de segurança.

Impacto

- Resultados indesejados da ocorrência de uma ameaça contra um bem, que resulta em perda mensurável para uma organização.

- Quase todo **risco** tem um impacto, embora de difícil previsão.

Risco

- É uma medida da **probabilidade da ocorrência de uma ameaça**.
- É a probabilidade do evento causador de perda ocorrer.
- Oficialmente, **um risco corresponde ao grau de perda**.

Ameaças, Riscos, Severidade

- Ameaças variam em severidade.
- **Severidade**: grau de dano que a ocorrência de uma ameaça pode causar.
- Riscos variam em probabilidade.

Tipos de Ameaças à Segurança

- Acesso não-autorizado
- Reconhecimento
- Recusa de Serviço
- Manipulação de Dados

Acesso Não-Autorizado

- Objetivo: obter acesso como administrador num computador remoto.
- Controlar o computador de destino e/ou acessar outros interligados.

Formas de Acesso Não-Autorizado

- Acesso inicial
- Com base em senhas
- Privilegiado
- Acesso secundário
- Permissão de acesso remoto
- Vulnerabilidades de programa
- Arquivos não autorizados

Reconhecimento

- Monitoramento de vulnerabilidades, serviços, sistemas ou tráfego de rede, no sentido de levantar informações visando um ataque futuro.

Formas de Reconhecimento

- Varreduras de porta

- Investigação:
  - observação passiva do tráfego de rede com um utilitário, visando padrões de tráfego ou capturar pacotes para análise e furto de informação.
  - *Snooping* de rede (*sniffing* de pacotes)

Recusa de Serviço

- Denial of Service (DoS)
- Tentativa de desativar ou corromper serviços, sistemas ou redes, no sentido de impedir o funcionamento normal.

Formas de Recusa de Serviço

- Sobrecarga de recurso
- Distributed Denial of Service
- Bombas de email

Manipulação de Dados

- Captura, alteração e repetição de dados através de um canal de comunicação.
- Falsificação de IP
- Repetição de sessão
- Repúdio

Falsificação de IP

- Ocorre quando um invasor da fora de uma rede, finge ser um computador confiável dentro da rede.

- O IP usado está dentro do intervalo da rede invadida, ou é usado um IP externo autorizado, confiável, e para o qual é disponibilizado acesso a recursos na rede.

Falsificação de IP

- Ocorre através da manipulação de pacotes IP.
- Um endereço IP de origem de um computador confiável, é falsificado para assumir identidade de uma máquina válida, para obter privilégios de acesso no computador invadido.

Segurança da Informação

- Somente **pessoas devidamente autorizadas** devem estar habilitadas a **ler**, **criar**, **apagar** ou **modificar** informações.

- **Controlar o acesso** às informações.

Controle de acesso: quatro requisitos

- (1) Manter confidenciais informações pessoais sensíveis (**privacidade**).
- (2) Manter **integridade** e precisão das informações e dos programas que a gerenciam.

Controle de acesso: quatro requisitos

- (3) Garantir que os sistemas, informações e serviços estejam disponíveis (acessíveis) para aqueles que devem ter acesso.

- (4) Garantir que todos os aspectos da operação de um SI estejam de acordo com as leis, regulamentos, licenças, contratos e princípios éticos estabelecidos.

Sobre requisitos

- Impedir acesso a alguns usuários (requisito 1) e autorizar fácil acesso a outros (requisito 3) requer **filtragem** muito bem feita.

- **Filtragem**, corresponde a introdução de **controles de segurança** que visem a reduzir riscos.

Exemplos de Ameaças aos Quatro Requisitos

Confidencialidade
Integridade
Acessibilidade
Leis / Ética

Ameaças

- Cavalos de Tróia
- Vírus
- Worms
- Vazamento de Informações
- Elevação de Privilégios
- Pirataria
- Falhas de Hardware
- Fraude

Ameaças

- Falsificação
- Backdoor
- Desfalque
- Incêndios ou Desastres Naturais

Ameaças

- Erros de Programadores
- Sniffers
- Entrada Inesperada
- Furto de informação

Cavalo de Tróia

- Programa que se apresenta executando uma tarefa e na realidade faz outra.
- Ameaça à: C, I, A.
- Prevenção: muito difícil.
- Detecção: pode ser muito difícil.
- Severidade: potencialmente muito elevada.

Vírus

- É um programa que infecta outros programas por modificá-los. A modificação inclui uma cópia do vírus, o qual pode então infectar outros.
- Ameaça à: I, A
- Prevenção: pode ser difícil.
- Detecção: normalmente imediata.
- Severidade: pode ser baixa ou potencialmente muito elevada.

Worms

- É um programa usa conexões de rede para se espalhar de sistema a sistema.
- Uma vez ativo, um *worm* pode comportar-se como a vírus, pode implantar programas cavalos de tróia ou realizar qualquer ação destrutiva.
- Um *worm* se replica usando facilidade de email, capacidade de execução remota e capacidade de *login* remoto.

Worms

- Ameaça à: Integridade, Acessibilidade.
- Prevenção: pode ser difícil.
- Detecção: normalmente imediata, através de antivírus.
- Severidade: pode ser baixa ou potencialmente muito elevada.

Pirataria de Software

- Cópia ilegal de software e documentação e re-embalagem para comercialização.
- Ameaça à: Leis / Ética
- Prevenção: muito difícil.
- Detecção: Pode ser difícil.
- Frequência: extremamente comum.
- Severidade: Potencialmente muito elevada.

Erros de Programadores

- Erros naturais de programação ao codificar, provocando *bugs* em proporções alarmantes.
- Ameaças à: C, I, A
- Prevenção impossível.
- Detecção: às vezes difícil
- Frequência: comum.
- Severidade: potencialmente muito elevada.

Sniffers

- Programas que podem ler qualquer aspecto de tráfego em uma rede, como por exemplo, capturando senhas, emails e arquivos.
- Ameaça à: Confidencialidade.
- Prevenção: impossível.
- Detecção: possivelmente detectados.
- Severidade: potencialmente muito elevada.

Desfalque

- Normalmente se refere a furto de dinheiro.
- Ameaça à: integridade e recursos.
- Prevenção: difícil.
- Detecção: pode ser difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Fraude

- Qualquer exploração de sistema de informação tentando enganar uma organização ou tomar seus recursos.
- Ameaça à: Integridade.
- Prevenção: difícil.
- Detecção: difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Falsificação

- Criação ilegal de documentos ou registros, intencionalmente produzidos como reais.
- Ameaça à: I e outros recursos.
- Prevenção: pode ser difícil.
- Detecção: pode ser difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Backdoor

- Um programa que é colocado numa máquina, como se fosse um serviço associado a uma porta, mas que tem a incumbência de fazer uma intrusão.
- Ameaça à: C. I, A.
- Prevenção: muito difícil.
- Detecção: possivelmente detectável.
- Severidade: potencialmente muito elevada.

Controles e Proteções

- **Controles** são procedimentos ou medidas que reduzem a probabilidade associada aos riscos.
- **Proteções** são controles físicos, mecanismos, ou políticas, que protegem os bens de ameaças.
- **Exemplos de proteção**: alarmes, senhas, controles de acesso.

Custos das Medidas

- Os gastos com segurança devem ser justificados como qualquer outro.

- A chave para selecionar medidas de seguranças adequadas é a habilidade de estimar a redução em perdas depois da implementação de certas proteções.

Custo-Benefício

- Uma análise de custo-benefício permite justificar cada proteção proposta.

- O custo das medidas de segurança deve ser sempre inferior ao valor das perdas evitadas.

Exposições

- **Exposições** são áreas da rede com probabilidade de **“quebra”** maior que outras.

Especialista em Segurança

- Apresentar **controles para modificar as exposições**, de modo que todos os eventos de determinada severidade tenham a mesma probabilidade.

- **Minimizar o custo de controles**, ao mesmo tempo, **maximizando a redução de exposições**.

Gerenciamento de Riscos

- Espectro de atividades, incluindo os controles, procedimentos físicos, técnicos e administrativos, que levam a soluções de segurança de baixo custo.

Gerenciamento de Riscos

- Procura obter as proteções mais efetivas contra ameaças intencionais (deliberadas) ou não intencionais (acidentais) contra um sistema computacional.

Gerenciamento de Riscos

- Tem quatro partes fundamentais.

- **Análise de Risco** (determinação de risco)
- **Seleção de Proteção**
- **Certificação e Credenciamento**
- **Plano de Contingência**

Análise Risco

- Pedra fundamental da gerência de riscos.
- Procedimentos para estimar a probabilidade de ameaças e perdas que podem ocorrer devido a vulnerabilidade do sistema.
- O propósito é ajudar a detectar proteções de baixo custo e prover o nível de proteção necessário.

Seleção de Proteção

- Os gerentes devem selecionar proteções que diminuem certas ameaças.
- Devem determinar um nível de risco tolerável e implementar proteções de baixo custo para reduzir perdas em nível aceitável.

Seleção de Proteção

- As proteções podem atuar de diversos modos:
  - Reduzir a possibilidade de ocorrência de ameaças.
  - Reduzir o impacto das ocorrências das ameaças.
  - Facilitar a recuperação das ocorrências das ameaças.

Seleção de Proteção

- A gerência deve focalizar áreas que têm grande potencial para perdas.

- As proteções devem ter boa relação custo-benefício, isto é, trazer mais retorno que os gastos com implementação e manutenção.

Certificação

- Podem ser importantes elementos da gerência de risco.

- Certificação é **verificação técnica** de que as proteções e controles selecionados são adequados e funcionam corretamente.

Credenciamento

- **Credenciamento** é a autorização oficial para operação, correções de segurança ou suspensão de certas atividades.

Plano de Contingência

- Eventos indesejados acontecem, independente da eficiência do programa de segurança.
- Permite uma resposta controlada que minimiza danos e recupera operações o mais rápido possível.

Plano de Contingência

- É um documento ou conjunto de documentos que permitem ações antes, durante, e depois da ocorrência de evento não desejado (desastre) que interrompe operações da rede.

Avaliando ameaças

- Exemplos (material escrito, distribuído em aula)
- Caracterizando ameaças.
- Examinar as ameaças possíveis à uma rede.

Capítulo 3

Preparação para Ataques:
Footprint e Fingerprint

Footprint

Busca detalhada de informações sobre o alvo para uma intrusão.

Footprint

- É a organização de idéias como um todo, tentando criar o melhor e mais completo perfil do alvo a ser atacado.
- O intuito é criar um perfil de uma máquina-alvo, para descobrir falhas que possam ser exploradas a partir de configurações e senhas padrões.

Footprint

- A partir do resultado do Footprint é que é traçado a estratégia de ataque.
- Um Footprint dura, enquanto for necessário.
- Pode ser colocado em prática de muitas formas, e é limitado apenas pela imaginação do atacante.

Objetivos comuns de Footprint

- Levantamento de Informações de Domínios:
  - Nomes de domínios.
  - Responsáveis pelos domínios
  - Servidores de domínios.
- Identificação do SO de máquina-alvo (Fingerprint).
- Descobrir subredes.
- Serviços TCP e UDP disponíveis.
- Topologia da rede.

Objetivos comuns de Footprint

- Contas de Email, FTP e outros serviços.
- Nomes de usuários e de grupos.
- *Banners* que identificam versões de serviços.
- Identificação de roteador e Tabelas de roteamento.
- Servidores ocultos por NAT (Network Address Translator).
- Endereços de e-mails.

Objetivos comuns de Footprint

- Informações de serviços SNMP mal configurados.
- Intervalos (Ranges) de IP de domínios.
- Estrutura de segurança quanto a existência de:
  - Firewalls
  - Sistemas IDS
  - Honeypots

Footprint

- Engenharia Social.
- Levantamento de Informações do Alvo: Whois ou comando host (Linux/Unix).
- Leitura de Banners para identificar servidores.
- Fingerprint do SO
- Enumeração dos Serviços e Versões
- Enumeração das Informações dos Serviços.
- Enumeração das Vulnerabilidades.

Engenharia Social

- É uma forma pessoal, ilícita, utilizada por crackers, para adquirir disfarçadamente, quaisquer informações fundamentais para a manutenção da segurança de um sistema.

Levantamento de Informações de Domínio

- Consulta na Base Whois (Internic).

  `whois <dominio>`

  `whois <ip/dominio>@registro.br`

  `fwhois <dominio>`

  `xwhois <dominio>` (ferramenta Linux)

- Procura na FAPESP (base do país).

  `http://registro.fapesp.br/`

  O domínio procurado está num provedor ou numa estação da própria empresa ???

Levantamento de Informações de Domínio

- Consulta na base DNS pelos comandos **`host`** ou **`dig`** ou **`nslookup`** (utilitário que pesquisa DNS), no Linux. Cada domínio possui uma base de dados DNS dos sub-domínios ali cadastrados.

Comando host

- Consultando toda a base DNS:

```
>host –l –v –t any <empresa>.com.br
```

- Descobrindo qual é o servidor de email:

```
>host –t mx <empresa>.com.br
```

- Descobrindo os IPs de servidores DNS:

```
>host –t ns <empresa>.com.br
```

- Verificando os CNAME (quais o servidores FTP, Web e outros):

```
>host –t CNAME <empresa>.com.br
```

Comando dig

- Buscando informações sobre o servidor DNS:

```
>dig –t ns <empresa>.com.br
```

- Buscando informações do registro MX:

```
>dig –t mx <empresa>.com.br
```

- **Buscando informações sobre o registro SOA:**

```
>dig –t soa <empresa>.com.br
```

Comando nslookup

- Varredura nas informações de um domínio (consultando CNAME)

- CNAME = nomes canônicos

```
>nslookup
Set type=cname
www.<empresa>.com.br
```

Levantamento de Informações de Domínio

- Levantamento de URL, através de consulta DNS, com a ferramenta IPZoner:

```
>./IPZoner –s <ip_de> -t <ip_para>
```

- Exemplo:

```
>./IPZoner –s 195.131.27.1 –t
             195.131.27.254
```

Levantamento de Informações de Domínio

- Levantamento de rotas de pacotes numa/entre redes (quais servidores e roteadores existem, a topologia da rede e identificar a estrutura de segurança), através do utilitário **`traceroute`** (Linux, Unix) ou **`tracert`** (Windows).

Rota de pacotes

- Exemplo: **traceroute vitima.com.br**

  router -> router -> máquina -> ... > servidor

- Exemplo: Traceroute analisando uma porta.

  traceroute –p25 192.168.0.2

  testa se há resposta na porta 25 (SMTP).

Footprint

Leitura de Banners

Leitura de Banners

- Identificando o servidor SMTP

  - Com Netcat na porta 25.

    ```
    > nc <ip> 25
    ```

  - Com a ferramenta SMTPScan que utiliza um banco de dados de perfil de servidores SMTP.

    ```
    > ./smtpscan inf.ufsc.br
    ```

Leitura de Banners - DNS

- Identificando a versão BIND em um servidor DNS:

  - Com a ferramenta dnsver.pl

```
>./dnsver.pl –t 50 –v <ip>
```

  - Com a ferramenta mig-named

```
>./mig-named –h <ip> -t 15 –d
```

Leitura de Banners - DNS

- Identificando versão BIND de DNS, porta 53, com a ferramenta grabbb :

```
>./grabbb -m -a 200. ... .
            -b 200. ... .254 53
 200. ... .103:53
 200. ... .199:53
 200. ... .3:53
>./mig-named –h 200. ... .103 –t 50 –d
  [200. ... .103]:[53] 9.2.1
> ...
>./mig-named –h 200. ... .3 –t 50 –d
 [200. ... .3]:[53] 9.2.1
```

- BIND (Berkeley Internet Name Domain) é uma implementação do Domain Name System (DNS)

Identificando SSH, Web

- Identificando servidores SSH, porta 22:

```
>./grabbb –m –a 200. ... .2 –b 200. ... .254 22

>./scanssh 200. ... .0/24 | grep –v refused |
 grep –v timeout | grep –v unreachable
```

- Identificando servidores Web:

```
>./grabbb –m –a 200. ... .104 –b 200. ... .254 80
200. ... .195:80:
200. ... .106:80:
>httpdtype 200. ... .195
...
>httpdtype 200. ... .106
...
```

Contramedidas – Leitura de Banners

- Utilizar a **obscuridade** por meio de eliminação de banners, restrição a consultas DNS e configurações que dificultem o levantamento das informações de banners.
- Obscuridade é complemento de segurança;
- Para agregar valor à segurança;
- Ver www.linuxsecurity.com.br
- Fazer atualizações de *patches*.

Footprint

Conceituando Portas

Protocolos TCP, ICMP, UDP, IP

Base para Scanners de Porta

Portas

- Sistema Operacional: kernel, serviços do sistema, serviços de comunicação (rede) e aplicações dos usuários, que podem se utilizar de serviços.

- A forma de identificação de um ponto de acesso de serviço de rede (SAP, OSI) é a porta de protocolo TCP/IP.

- Sockets TCP/IP = (IP, portas)

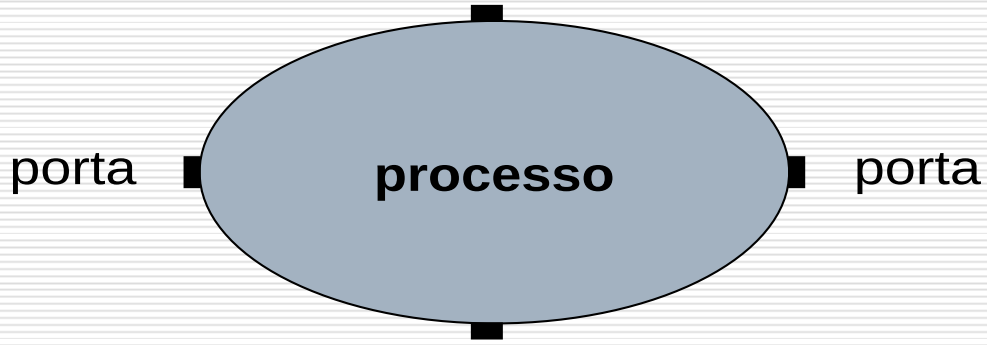
Portas

- A porta é a unidade que permite identificar o tráfego de dados destinado a diversas aplicações.

- A identificação única de um processo acessando os serviços de rede TCP/IP é o *socket* TCP/IP, formado pelo par IP da máquina e a porta(s) usada(s) para acessar um serviço(s) de rede utilizado(s) por uma aplicação.

Portas simultâneas

- Cada processo pode utilizar mais de uma porta simultaneamente (entrada, saída), mas, em um dado instante, uma porta só pode ser usada por uma aplicação.



Portas

- Uma aplicação que deseje utilizar os serviços de rede deverá requisitar uma ou mais portas para realizar a comunicação.

- A mesma porta usada por uma aplicação pode ser usada por outra, desde que a primeira tenha liberado aquela de utilização.

Portas

- A forma de utilização de portas mostra uma distinção entre a parte cliente e a parte servidora de uma aplicação TCP/IP.

Portas

- Uma aplicação-servidora deve utilizar um número de porta bem conhecido, de modo que um cliente qualquer, querendo utilizar os serviços do servidor, tenha que saber apenas o endereço IP da máquina onde o serviço está sendo executado.

Portas

- A aplicação cliente pode utilizar um número de porta qualquer.

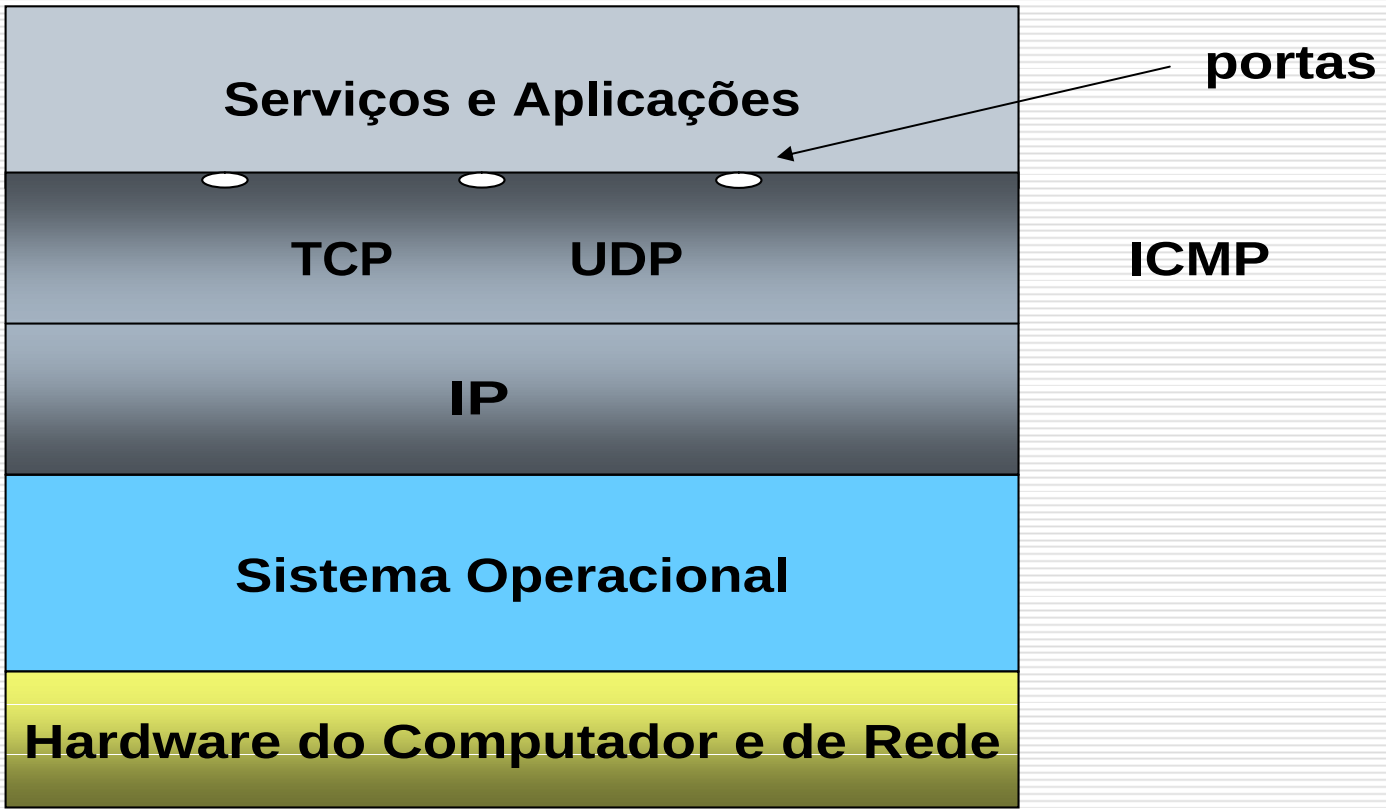
- Os números de porta de 1 a 1023 são números bem conhecidos para serviços de rede, atribuídos pela IANA (Internet Assigned Numbers Authotity).

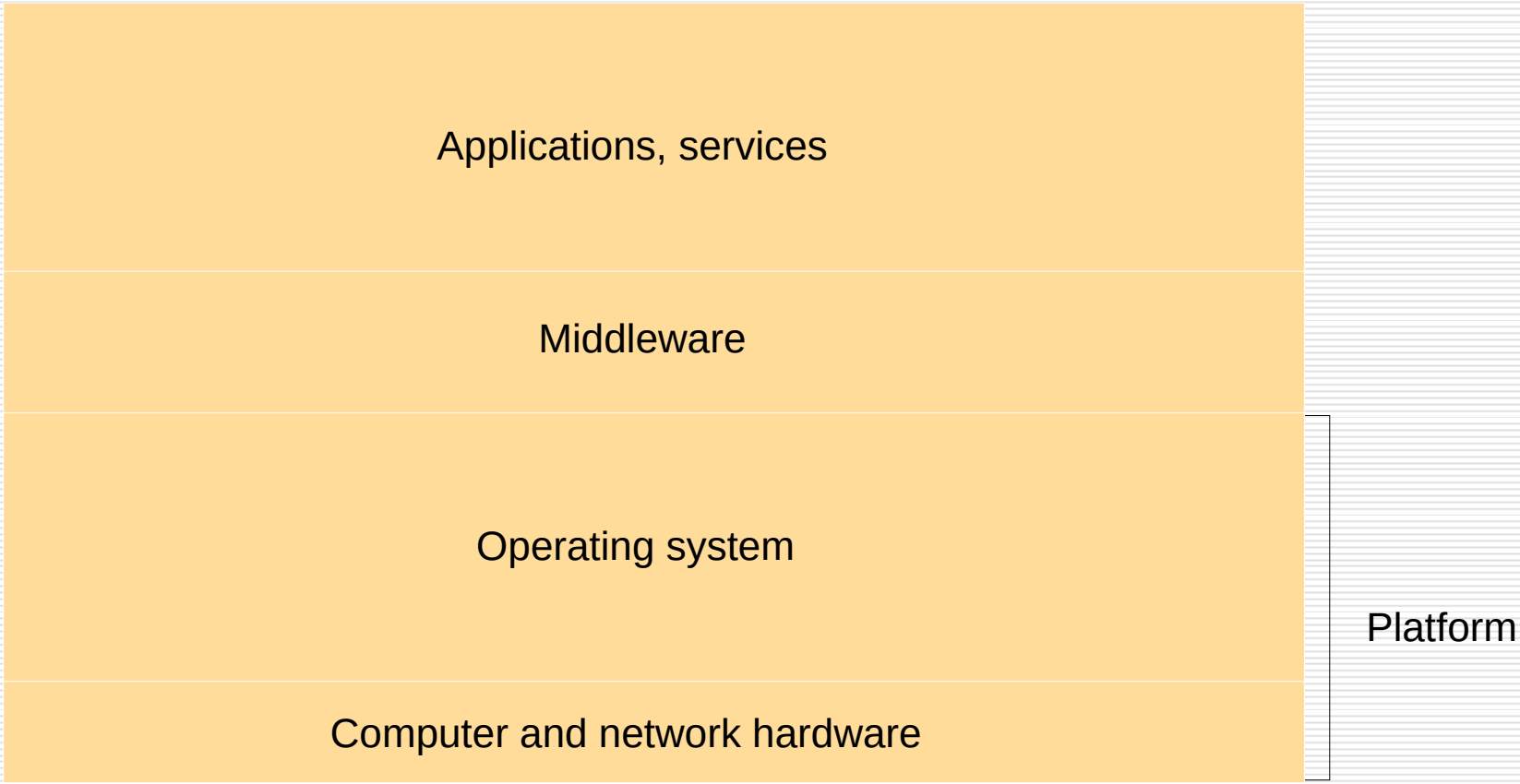
Portas

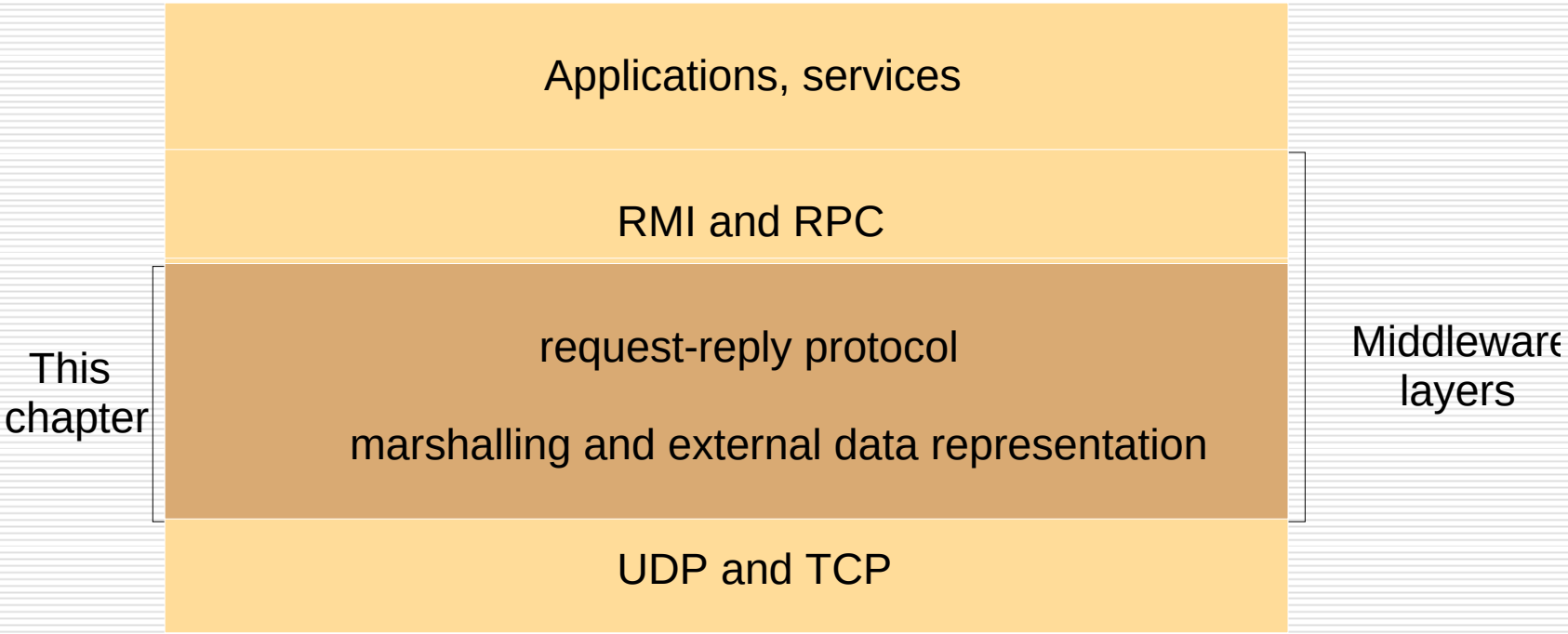
- Os números de 1024 a 65535 podem ser atribuídos para outros serviços, e são geralmente usados pelos programas-cliente de um protocolo.

- As portas servem para identificar o tipo de aplicação que gerou as mensagens de dados, e para qual tipo de aplicação as mensagens de dados devem ser entregues.

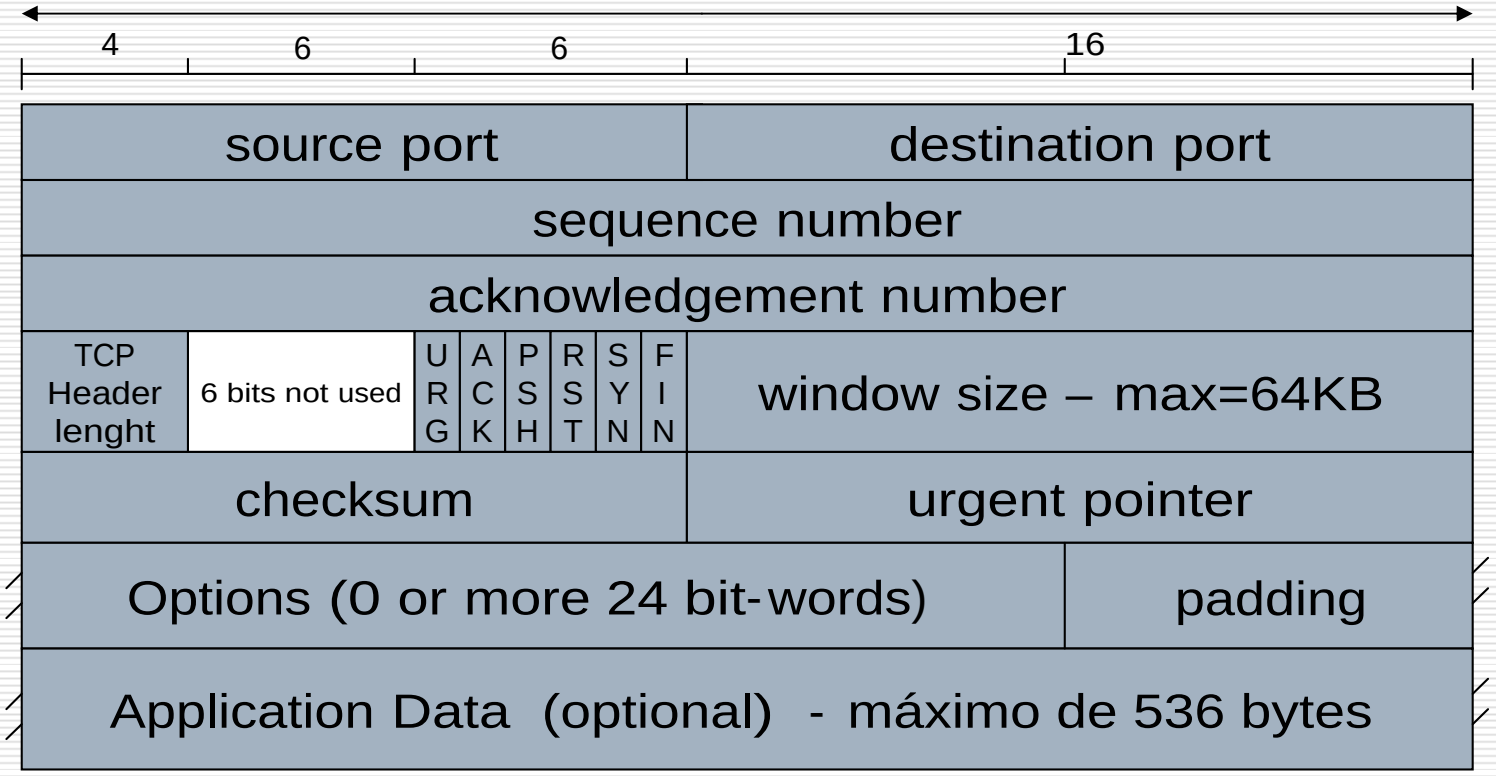
Portas TCP


Serviços e Aplicações
portas
TCP
UDP
ICMP
IP
Sistema Operacional
Hardware do Computador e de Rede


Applications, services
Middleware
Operating system
Computer and network hardware
Platform


Applications, services
RMI and RPC
request-reply protocol
marshalling and external data representation
UDP and TCP
This chapter
Middleware layers

Protocolo TCP – Segmento TCP

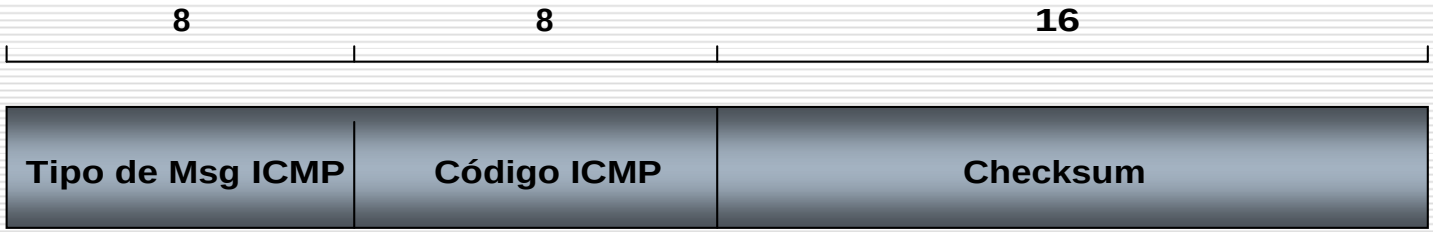


TCP – Bits de Controle

Bit	Significado
URG	O campo indicador Urgente é válido.
ACK	O campo número de confirmação é válido.
PSH	Força a entrega de dados.
RST	Reiniciar a conexão.
SYN	Sincronismo, determina o número de sequência inicial.
FIN	O transmissor chegou ao fim de seus dados.

Protocolo ICMP

- Encapsulado no protocolo IP, mas não é um protocolo de alto nível (TCP, UDP).



Valor	Alguns Tipos de mensagem ICMP
0	**Resposta à mensagem de Echo**
3	**Aviso de destino inalcançável**
4	Redução da Velocidade de Transmissão
5	Solicitação de Redirecionamento
8	**Mensagem de Echo**
11	Tempo de Vida Excedido (Time To Live)
12	Problema nos parâmetros
...	**...**

Bits de Varredura

- Varreduras usando TCP usam os bits de controle:

  SYN, ACK, RST, FIN, URG, PSH

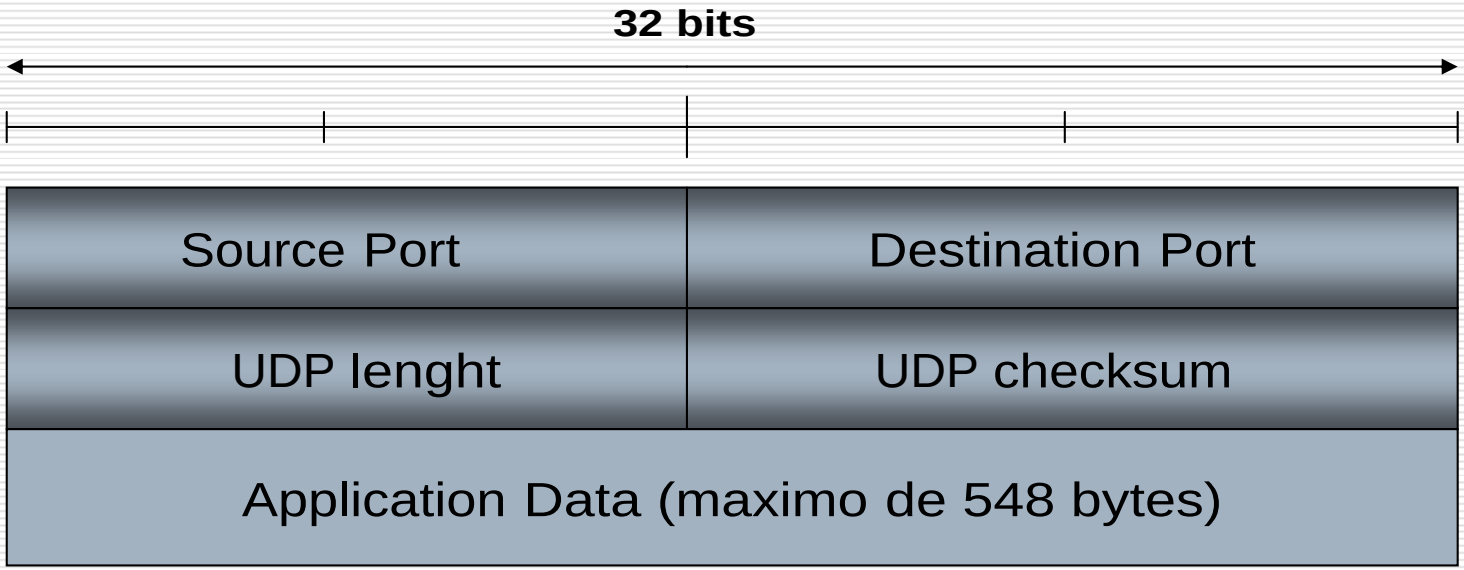
- Varreduras usando ICMP usam pacotes IP contendo ICMP tipo 3.

Protocolo UDP

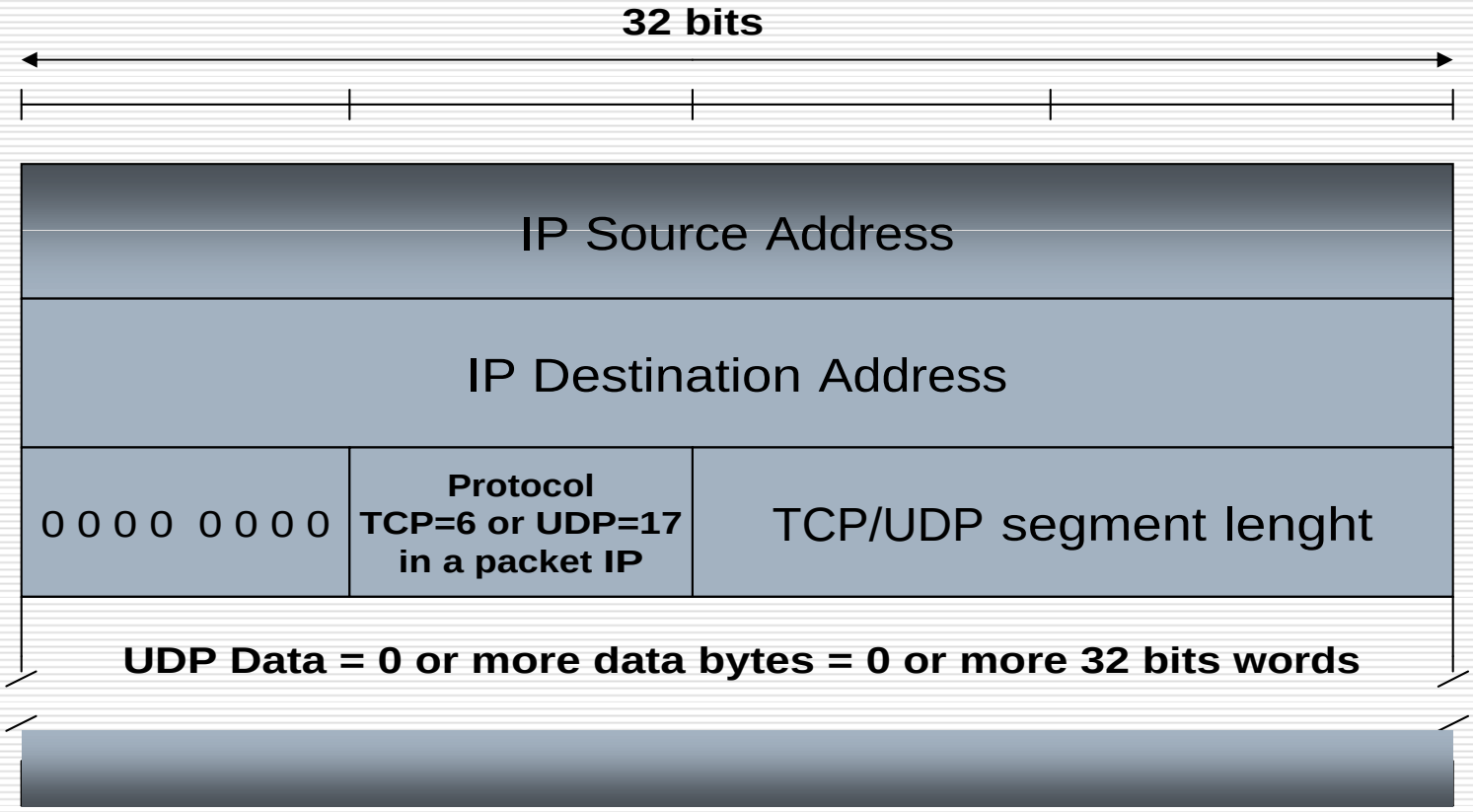
- *Suite* de protocolos Internet.
- User Datagram Protocol (*RFC 768).*
- Um protocolo de transporte sem conexão.
- Provê um modo de aplicações enviarem datagramas UDP encapsulados em pacotes IP.
- Muitas aplicações que têm um *request* e um *response* usam UDP (Echo, Whois, DNS, ...).

O segmento UDP

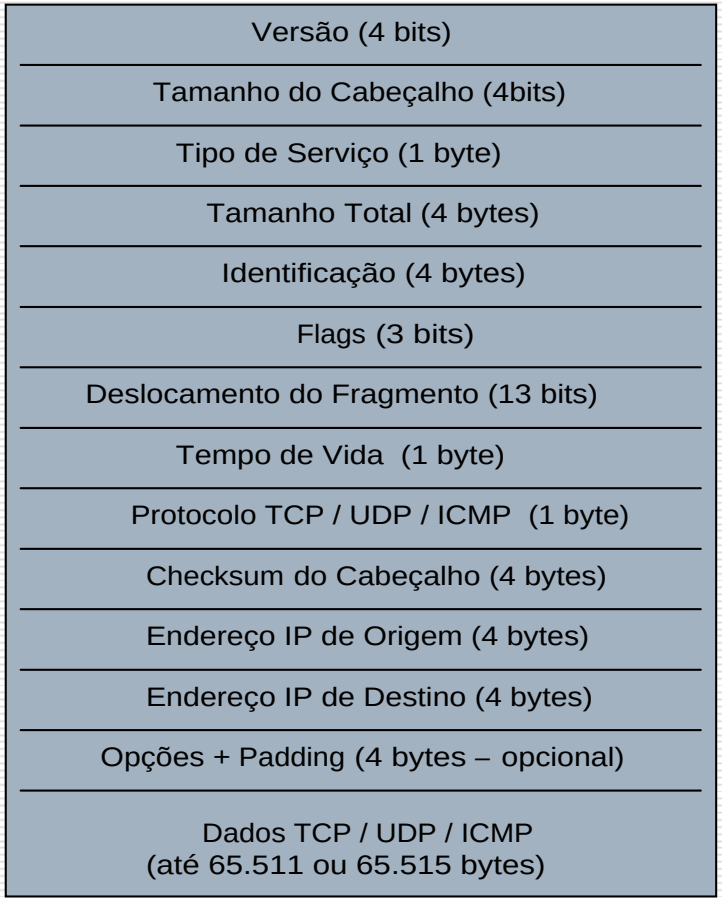
- Um segmento UDP consiste de um cabeçalho de 8 bytes seguido por dados da aplicação.



O Pseudo Cabeçalho TCP/UDP

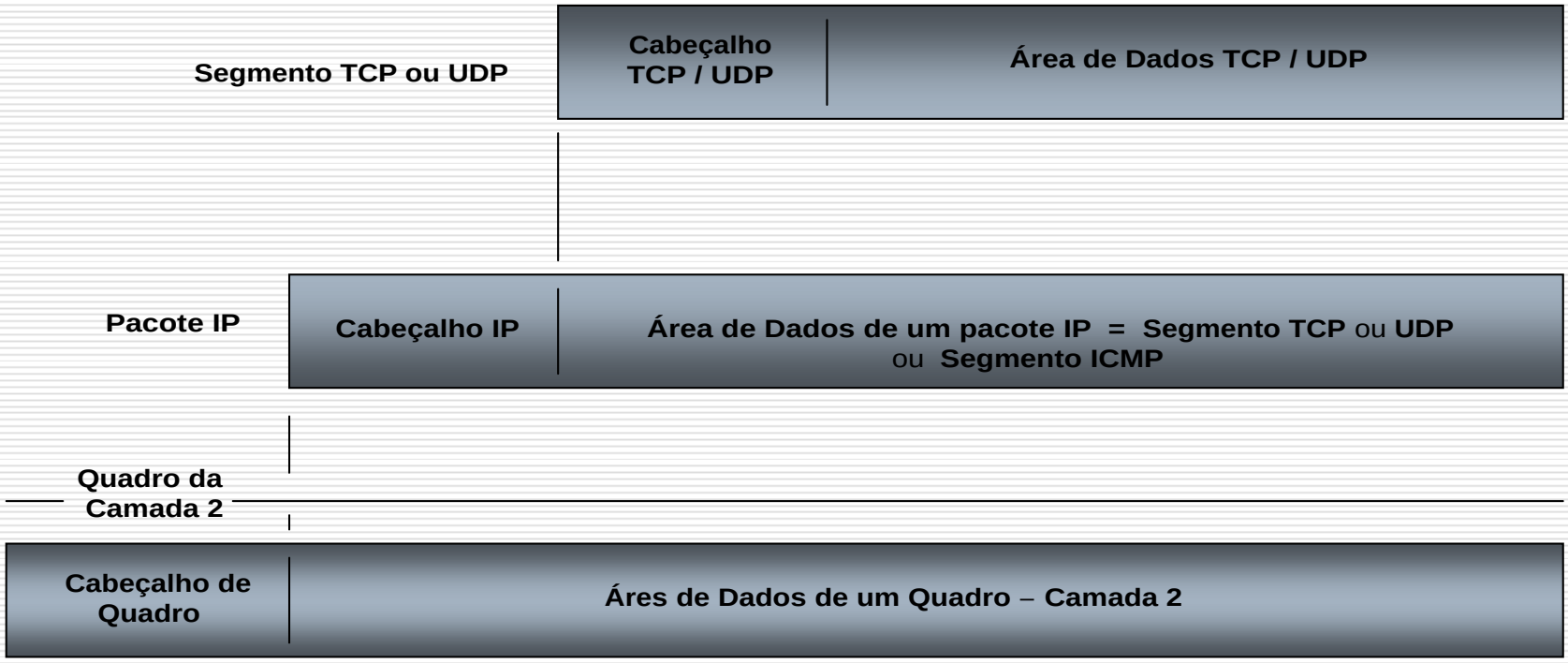


Estrutura de um pacote IPv4



← **Segmentos: TCP ou UDP ou ICMP**

Encapsulamento de Segmentos



Pseudo Cabeçalho

- Existe, apenas, apara efeito de cálculo do checksum.
- **Não é transmitido**.
- O checksum do TCP é calculado da mesma forma que no UDP.
- O ckecksum é calculado somando-se o cabeçalho, o pseudo-cabeçalho e o campo de dados.

Footprint

Enumeração dos Serviços e Versões

Scanners de Porta

Scanners de Portas

- Pesquisam faixas de endereços IP.
- Descobrem portas abertas (que têm serviços rodando).
- Informações sobre o Sistema Operacional de uma máquina alvo (Fingerprint).

Scanner Nmap

- Nmap (http://www.nmap.org)
- Código Aberto.
- Licença GNU GPL.
- Auditoria de Sistemas.
- Pode ser usado para **Footprint** e **Fingerprint**.

Mostrando o Nmap

```
# /usr/local/nmap -O ganassi

Starting nmap V. 2.53 (www.insecure.org/nmap/)
Interesting ports on ganassi (10.8.10.231):
(The 1515 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
```

Footprint - Técnicas de **Fingerprint**

Técnica de levantamento de informações para **identificar o sistema operacional** da máquina-alvo.

Fingerprint

- Informação fundamental para um invasor buscar uma possibilidade de intrusão.
- Técnicas Clássicas.
- Técnicas mais elaboradas.
- Crackers e Script Kiddies utilizam ferramentas: **Queso**, **Nmap**.
- **Queso** foi projetada para fingerprint.
- **Nmap** pode fazer fingerprint na pilha TCP do host-alvo (usando UDP, TCP, ICMP).

O conceito de Intrusão

- Análise da **Vulnerabilidade** (descobrir o melhor caminho para chegar até a invasão).
- Preparação das **Ferramentas** (constrói ou escolhe as ferramentas para a invasão).
- **Ameaça** ou Tentativa (quando o invasor pula o muro).
- **Ataque** (concretiza o arrombamento).
- **Invasão** (quando obtém sucesso).

Idéia básica para uma intrusão

- Ao **determinar qual SO** está rodando, o invasor pode **organizar suas ferramentas** de acordo com a plataforma-alvo.

- O invasor pode ter como objetivo, **"rootear"** a máquina-alvo, e deve sempre saber as **diferenças dos formatos binários** de cada sistema.

Idéia básica para uma intrusão

- O invasor tem em mente que, ao saber o SO de um host-alvo, ele pode **visar um serviço** do respectivo sistema,

- descubrir uma vulnerabilidade desse serviço, e tendo em mãos um ***exploit*** **funcional para explorar esse serviço**,

- ele terá uma oportunidade que lhe permitirá **"rootear"** (assumir o perfil de administrador com senha de root).

Investidas Errôneas

- Um investida errônea sobre o serviço pode tirá-lo do ar e/ou chamar a atenção do administrador.

- Casos freqüentes de queda de serviços, por razões desconhecidas: verificação dos arquivos de *log* do servidor, Firewall e IDS.

Formas de Fingerprint

- Técnicas Clássicas

- Fingerprint com **Cheops**
- Fingerprint com **Nmap** ou **Nmap** e **Nift**

- UDP Echo

- TCP Syn
- TCP Echo
- TCP Ack

- ICMP Echo

- Usar ferramentas como **snmpwalk** ou **LANguard** sobre servidores habilitados com SNMP e configurados de forma padrão.

Fingerprint com **Cheops**

- **Cheops** é um programa mapeador de redes pequenas, que tem vários recursos, entre eles, a capacidade de fazer *fingerprint*.

- Não identifica todos os sistemas remotos ...

Fingerprint com **Nmap**

- *Fingerprint* através da Pilha TCP/IP

  Extrair informações de uma máquina através das características implementadas em sua pilha TCP/IP.

Fingerprint com Nmap

- nmap–os-fingerprint**s (nome do arquivo dos perfis de SOs)**

- **Para usar o recurso de Fingerprint, utilizar a opção "-O":**

  nmap **–O** <ip>

- **Fingerprint em uma única porta:**

  nmap –O **–p80** <ip>

- **Fingerprint com modo de varredura máxima:**

  nmap –O –p21 **–osscan_guess** <ip>

- nmap **–n** –p80 **–PO** -O --osscan_guess <ip>
- nmap –n –P6001 –PO –O –osscan_guess localhost

Fingerprint com **Nift**

- **Nift** é uma **ferramenta front-end** para **Nmap** e outas ferramentas.
- Apresenta uma **interface gráfica**.
- Tem recursos para varreduras de serviços, fingerprint e varredura ICMP.
- O objetivo de **Nift** é identificar o alvo e enumerar serviços.
- Download de Nift em: ....

Fingerprint com **Nmap**

- Descobrir quais os respectivos SOs.

  nmap –sS –p80 –O –v <host>
  nmap –sS –p80 –O –osscan_guess –v <host>

- Fazendo um teste numa corporação de nome empresa. O parâmetro <empresa>.log é um arquivo de log.

  nmap –sS –F –o <empresa>.log –v –O www.<empresa>.com/24

  Este comando faz SYN scan nas portas conhecidas em (/etc/services), “loga” o resultado no arquivo <arquivo>.log e em seguida faz um scan do SO e um scan na classe “C”. Veja o resultado: S*ite* e o SO.

Fingerprint com Nmap

- Quando é anunciado um “bug” de segurança, esses invasores podem ir a um *site* de *exploits* em busca de uma ferramenta para explorar tal “bug”.

- “modus operandi do script kiddie”

Footprint

Técnicas de Varreduras

Enumeração dos Tipos de Serviços e Versões

Varredura de Portas → Serviços

Serviços → Varredura de Vulnerabilidades

Enumeração

- Extração de informações do ambiente-alvo, como os serviços de rede TCP e UDP, que requerem portas.

Enumeração dos Tipos de Serviços Disponíveis e Versões

- Varreduras de Portas Clássicas
- Varreduras TCP, UDP, ICMP.

- Port Scanners
  - NetStat (Windows)
  - Netcat
  - Nmap
  - Amap (ideal para leitura de *banners*)
  - Blaster
  - Hping2

- **Intrusão** ou para **Auto-Monitoramento**

Footprint

Enumeração de Informações dos Serviços

Varreduras a partir de Serviços

- SMTP Scan (levanta dados a partir do serviço SMTP).
- SMB Scan (compartilhamento Windows, em UNIX, provido pelo Samba).
- RPC Scan (levanta dados a partir do serviço de RPC)

- **Intrusões** ou **Auto-Monitoramento**

Vulnerabilidades

- São as falhas de segurança em um sistemas de software ou de hardware que podem ser exploradas para permitir a efetivação de uma intrusão.

Footprint

Descoberta de vulnerabilidades

Um scanner de vulnerabilidades

- Nessus (http://www.nessus.org)
- Scanner de segurança que identifica vulnerabilidades, e tenta testar as encontradas.
- Administração Remota.

Varredura de Vulnerabilidades

- Enumeração das falhas e configurações padrões dos serviços.

- Serve para concretizar **ataques**:

  são usados *Exploits* (ferramentas para a exploração de vulnerabilidades) para os respectivos serviços levantados.

- Ou para realizar **Auto-Monitoramento**

Mostrando o Nessus

```
# nessus -T text localhost 1241 noorder targetfile outfile
```

Mostrando o Nessus

```
Nessus Scan Report
------------------

SUMMARY

  - Number of hosts which were alive during the test : 1
  - Number of security holes found : 2
  - Number of security warnings found : 15
  - Number of security notes found : 1

TESTED HOSTS

  192.168.0.90 (Security holes found)
```

Mostrando o Nessus

```
DETAILS

+ 192.168.0.90 :
  . List of open ports :
    o unknown (161/udp) (Security hole found)
    o unknown (32779/udp) (Security warnings found)
    o unknown (32775/tcp) (Security warnings found)
    o unknown (32776/udp) (Security warnings found)
    o unknown (32778/udp) (Security warnings found)
    o unknown (32774/udp) (Security hole found)
    o unknown (32777/udp) (Security warnings found)
    o unknown (32780/udp) (Security warnings found)
    o unknown (32775/udp) (Security warnings found)
    o lockd (4045/udp) (Security warnings found)
    o unknown (32781/udp) (Security hole found)

. Vulnerability found on port unknown (32774/udp) :

     The sadmin RPC service is running.
     There is a bug in Solaris versions of
     this service that allow an intruder to
     execute arbitrary commands on your system.

     Solution : disable this service
     Risk factor : High
```

SUSSEN - Interface para Nessus

- Um cliente não oficial para o Nessus, denominado **SUSSEN**:

- Integração com MySQL Server V4.0, como backend.
- Suporte a múltiplos servidores Nessus.
- Suporte a geração de múltiplos relatórios.
- Baseado em GNOME/Gtk+ 2.2 APIs.

SUSSEN - Interface para Nessus

- Integração com ajuda de manual on-line.
- Política de gerenciamento de plugins e scanners de porta.
- Suporte a internacionalização e localização.
- Suporte à XML.
- http:// .....

Referências para Scanners

- Noordergraaf, Alex. Enterprise Server Products. How Hackers Do It: Trick, Tools and Techniques. Sun BluePrints™ OnLine – May, 2002.
- http://www.sun.com/blueprints
- CERT: http://www.cert.org.
- Nessus: http://www.nessus.org
- Nmap: http://www.nmap.org
- Serafim, Vinícius da Silveira. Atacantes: Suas principais técnicas e ferramentas. Gseg - UFRGS. http://www.inf.ufrgs.br/~gseg/
- CVE: http://cve.mitre.org.