FIAP ON

CYBERSECURITY

CARACTERÍSTICAS E *VULNERABILIDADES*

OSMANY DANTAS RIBEIRO DE ARRUDA

5

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

5 CARACTERÍTICAS E VULNERABILIDADES

5.1 As redes computacionais e os serviços básicos

É notório que, desde há muito, as redes e os sistemas computacionais passaram a ser parte obrigatória da infraestrutura das empresas, dentre outras razões, dadas a agilidade e a escalabilidade cada vez mais necessárias e exigidas pelo negócio, tornando, dessa maneira, a tecnologia da informação e comunicações alguns de seus prestadores de serviços mais requisitados.

Tomem-se como exemplos triviais o serviço de e-mails, como veículo para troca de mensagens e arquivos entre pares remotos, e o sistema de resolução de nomes de domínio (Domain Name Service – DNS): qual seria o potencial impacto para o negócio, caso uma importante proposta de orçamento para um cliente ou, ainda, a documentação necessária à participação em uma importante concorrência não pudessem ser entregues no prazo em decorrência da descontinuidade do serviço de e-mails, por qualquer motivo que seja, como, por exemplo, em decorrência da disrupção do serviço DNS?

Esse exemplo, embora bastante trivial, já permite observar claramente ao menos dois pontos: (a) a relevância dos serviços de rede é cada vez maior como auxiliar na concretização dos objetivos de negócio e, ainda, (b) pode haver uma intrínseca ligação entre serviços independentes.

Um dos fatores que certamente melhor justificam os investimentos nas redes, especialmente as locais (LAN), recai sobre o compartilhamento de recursos, tais como acesso à internet, armazenamento de arquivos, envio/recebimento de mensagens eletrônicas e sincronização de relógios, dentre muitos outros; todos, de uma forma ou de outra, contribuindo à sua maneira para que a informação sirva adequadamente à empresa.

5.1.1 Uma topologia de referência

Considere-se como exemplo a topologia proposta na Figura “Topologia de referência”.

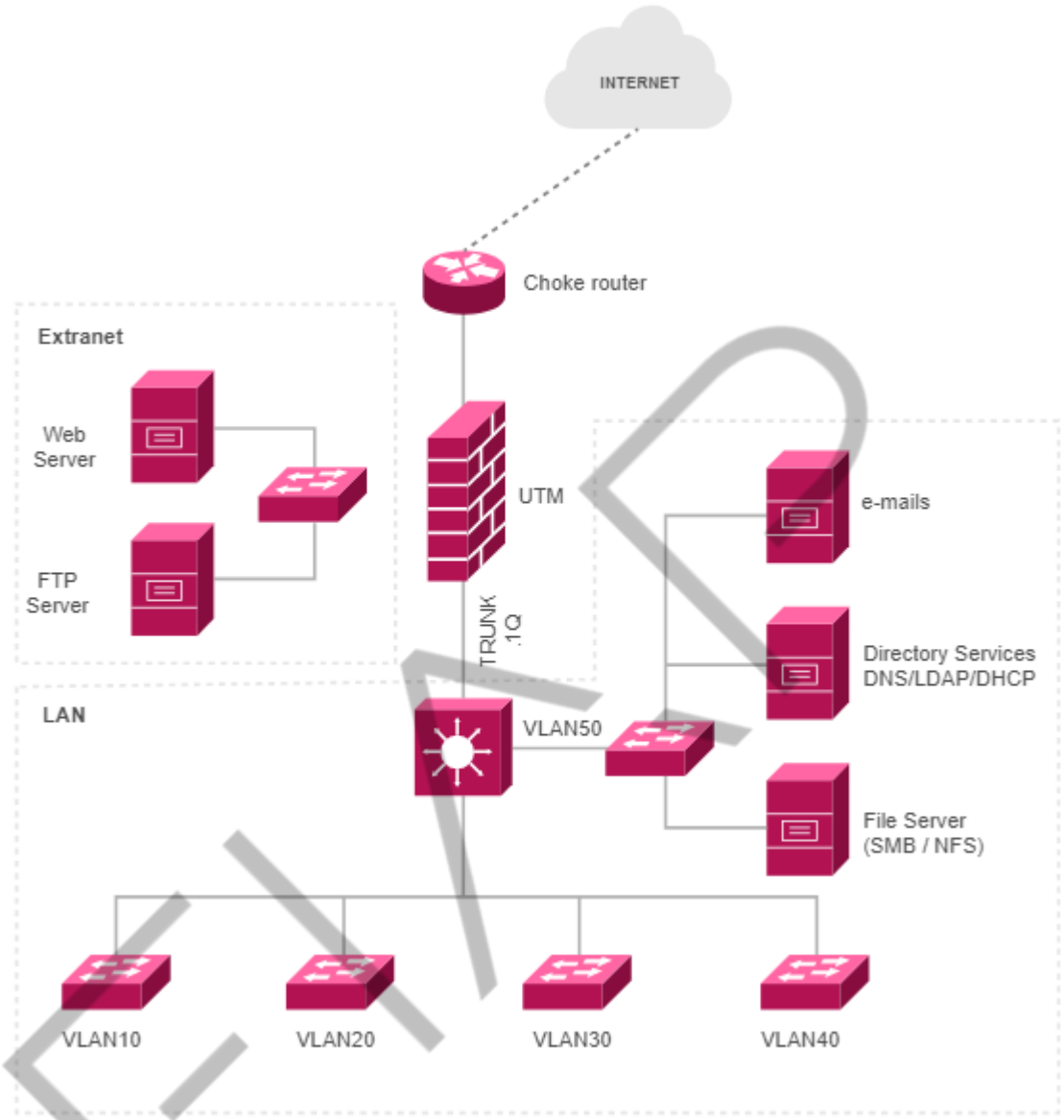

Figura 5.1 – Topologia de referência
Fonte: Elaborado pelo autor (2020)

Essa topologia de referência representa um ambiente hipotético, no qual os serviços de e-mail, de diretório (*Directory Services*) e compartilhamento local de arquivos são disponibilizados à rede local (LAN), tendo-se ainda disponível um serviço para troca de arquivos e de conteúdo web estático com a rede não confiável (internet), por intermédio de uma Extranet bastante simples.

Cada um desses serviços é implementado por um ou mais protocolos específicos da camada de APLICAÇÃO do TCP/IP (camada 7 do modelo OSI), definindo-se protocolo como um conjunto de regras que governa a comunicação de dados, determinando o que, como e quando deverá ser comunicado (Forouzan, 2008).

A Figura” Principais protocolos de comunicação e serviços” ilustra o posicionamento de alguns dos principais protocolos da camada de APLICAÇÃO da pilha TCP/IP, aplicáveis ao cenário da Figura “Topologia de referência”.

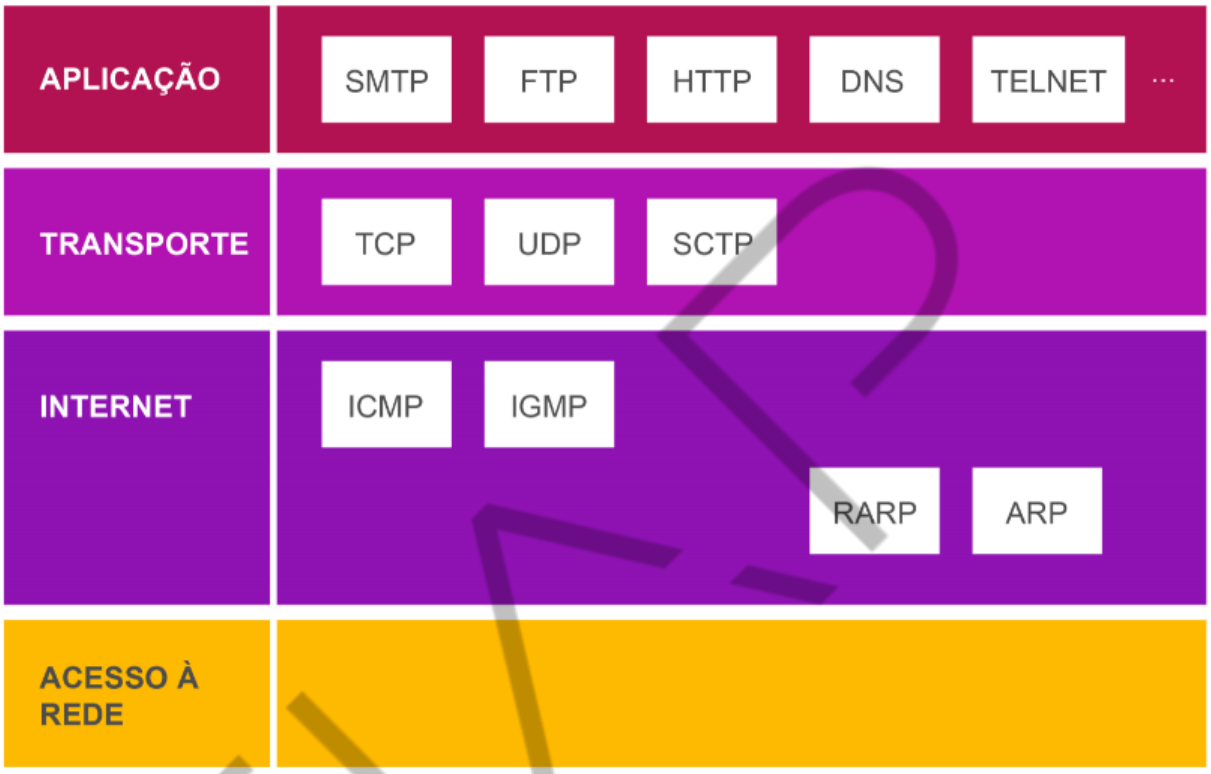

Figura 5.2 – Principais protocolos de comunicação e serviços
Fonte: Adaptado de Forouzan (2008)

5.1.2 O estabelecimento da conexão

Alguns dos protocolos de serviço, como, por exemplo, o FTP e o HTTP, exigem o prévio estabelecimento de uma conexão (camada de TRANSPORTE) a fim de poder operar. O estabelecimento de uma conexão entre dois *hosts* é efetivado mediante uma troca de informações entre eles, executada em três fases, a fim de identificarem um ao outro e de estabelecerem o sincronismo necessário à troca de pacotes enquanto a conexão persistir. Esse processo denomina-se THREE-WAY HANDSHAKE e equivale ao aperto de mão inicial entre duas pessoas, antecedendo o início da conversação; também é resumidamente definido por Blank (2004) como um diálogo de três fases, iniciado pelo **TCP** para configurar uma conexão entre hosts.

Retomando-se o cenário da Figura “Topologia de referência”, considere-se agora que o usuário de uma estação de trabalho qualquer da rede requisite uma página html ao servidor web na extranet. Com a ajuda do Wireshark, o diálogo entre esses dois hosts para atendimento da referida requisição foi capturado, consistindo do exposto na Figura “Diálogo requisição/resposta”.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.0.0.1	TCP	74	59520 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
2	0.000528	10.0.0.1	10.0.0.2	TCP	74	80 → 59520 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.001122	10.0.0.2	10.0.0.1	TCP	66	59520 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSv
4	0.001565	10.0.0.2	10.0.0.1	HTTP	319	GET / HTTP/1.0
5	0.002515	10.0.0.1	10.0.0.2	TCP	66	80 → 59520 [ACK] Seq=1 Ack=254 Win=6912 Len=0 TS
6	0.013062	10.0.0.1	10.0.0.2	HTTP	1152	HTTP/1.1 200 OK (text/html)
7	0.013288	10.0.0.1	10.0.0.2	TCP	66	80 → 59520 [FIN, ACK] Seq=1087 Ack=254 Win=6912
8	0.013730	10.0.0.2	10.0.0.1	TCP	66	59520 → 80 [ACK] Seq=254 Ack=1087 Win=31488 Len=
9	0.015295	10.0.0.2	10.0.0.1	TCP	66	59520 → 80 [FIN, ACK] Seq=254 Ack=1088 Win=31488
10	0.015739	10.0.0.1	10.0.0.2	TCP	66	80 → 59520 [ACK] Seq=1088 Ack=255 Win=6912 Len=0

Figura 5.3 – Diálogo requisição/resposta
Fonte: Elaborado pelo autor (2020)

A Figura “Diálogo requisição/resposta” permite observar que os três primeiros pacotes são os responsáveis pela negociação que estabelecerá a conexão (por parte do protocolo TCP) necessária ao atendimento da requisição feita pelo cliente (host com endereço IP 10.0.0.2) ao servidor (host com endereço IP 10.0.0.1), por intermédio do protocolo HTTP, possibilitando, ainda, representar-se graficamente esse processo conforme a Figura “Estabelecimento da conexão”.

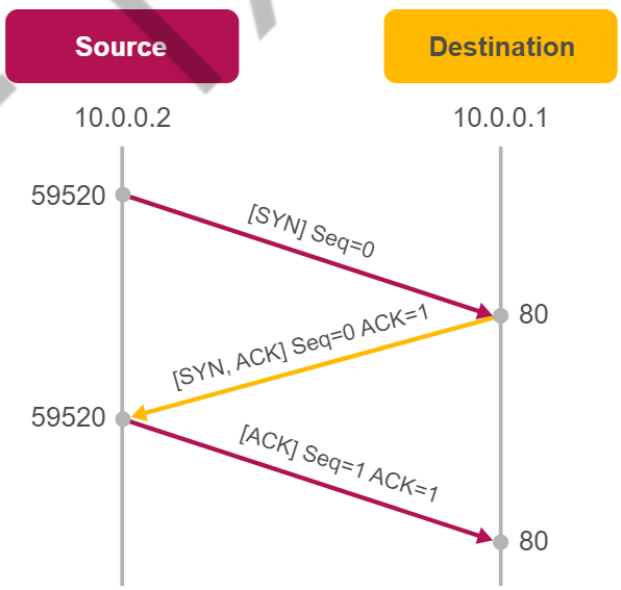

Figura 5.4 – Estabelecimento da conexão
Fonte: Elaborado pelo autor (2020)

A Figura “Estabelecimento da conexão” representa o THREE-WAY HANDSHAKE, a partir do qual é possível observar haver sido o primeiro pacote enviado

pelo host 10.0.0.2 (cliente) a partir de uma porta desprivilegiada (59520), com destino à porta 80 (*well-known port*) do host 10.0.0.1 (servidor), via protocolo TCP, caracterizando-se dessa forma uma requisição para o serviço HTTP no servidor (web).

Esse pacote enviado ao servidor (1), leva a *flag* SYN (cabeçalho TCP) habilitada, caracterizando assim uma solicitação de conexão, mais o valor zero no campo SEQUENCE NUMBER.

Por sua vez, (2) o servidor responde com outro pacote, também com a *flag* SYN habilitada; sinalizando, ainda, o sucesso no recebimento do pacote enviado pelo cliente, por meio da *flag* ACK, e carregando o campo ACKNOWLEDGE NUMBER com o valor 1 (valor do campo SEQUENCE NUMBER do cliente + 1). Por fim, (3) o cliente responde ao servidor com novo pacote com a *flag* ACK habilitada, por sua vez, também acrescendo de um os valores dos campos SEQUENCE NUMBER e ACKNOWLEDGE NUMBER, sendo então estabelecida a conexão e, dessa maneira, é possível ao protocolo HTTP atender à requisição de conteúdo feita pelo cliente.

5.2 protocolos de comunicação e serviços

5.2.1 Protocolo HTTP (Hypertext Transfer Protocol)

O protocolo **HTTP** opera com base em requisições e respostas no modelo cliente-servidor; portanto, quando um navegador (cliente) requisita uma página a um servidor web, ele a enviará ao cliente, em resposta à solicitação feita. Em utilização desde 1990, a versão HTTP/1.0 (que não é a primeira versão do protocolo) foi desenvolvida em resposta à necessidade de transferência de dados também em formatos diferentes do texto ASCII. Em sua versão HTTP/1.1, métodos adicionais foram acrescentados ao protocolo, permitindo sua utilização com outros protocolos, como, por exemplo, FTP e SMTP.

Os navegadores web se utilizam predominantemente do método GET, para recuperar dados do servidor, e do método POST, para solicitar ao servidor que aceite os dados a serem transmitidos, como, por exemplo, o *upload* de um arquivo. O HTTP é também um protocolo ***stateless*** e ***connectionless***, o que resumidamente significa que cada requisição feita pelo cliente ao servidor por intermédio dele será tratada isoladamente, encerrando-se a conexão ao final de cada sessão requisição/resposta,

sem que qualquer informação a respeito dessa conexão venha a ser preservada por nenhum dos dois interlocutores.

Os pacotes 4 (requisição) e 6 (resposta) na Figura “Diálogo requisição/resposta” demonstram a transação do protocolo HTTP para atendimento à solicitação do cliente, sendo que, observando-se também os pacotes subsequentes, é possível verificar, como anteriormente exposto, que esse protocolo não estabelece a conexão – dependendo do TCP para fazê-lo, sendo essa conexão finalizada assim que a requisição for respondida.

5.2.2 Protocolo FTP (File Transfer Protocol)

O protocolo FTP destina-se à troca de arquivos (predominantemente) na internet, podendo operar de dois modos diferentes: ativo ou passivo.

Apesar de possuir mecanismos para autenticação do usuário, estes são frágeis na medida em que, analogamente ao conteúdo dos arquivos trafegados por esse protocolo, também as credenciais do usuário (*username* e senha) trafegam pela rede em *plain text*. O protocolo FTP estabelece duas conexões distintas, porém relacionadas entre si, para operar: uma de controle e outra de dados.

A conexão de controle inicia e finaliza cada sessão, permanecendo ativa enquanto a sessão persistir, tendo como função gerenciá-la (por exemplo, enviando comandos ao servidor, ou as credenciais para autenticação). Por sua vez, a conexão de dados estabelece o canal por onde trafegarão os arquivos a serem baixados, ou transferidos, pelo usuário. Essa maneira particular de operação, baseada em duas conexões distintas, faz com que o protocolo FTP seja considerado *out-of-band*, diferentemente, por exemplo, do protocolo HTTP, considerado *in-band*.

O protocolo FTP se vale do TCP para estabelecimento das conexões necessárias ao seu funcionamento, sendo que, quando operando em modo ativo, utiliza-se duas portas bem conhecidas: 20 (FTP DATA) e 21 (FTP COMMAND), enquanto no modo passivo, utiliza apenas a porta 21.

5.2.2.1 O protocolo FTP em modo Ativo

O modo ativo é, sob certo aspecto, ainda mais inseguro que o modo passivo, na medida em que viola o modelo cliente-servidor, forçando esse último a iniciar a conexão de dados com o cliente.

A Figura “FTP operando em modo ativo” ilustra a negociação do protocolo FTP, para estabelecimento dos canais de comando e transferência de dados, em modo ativo.

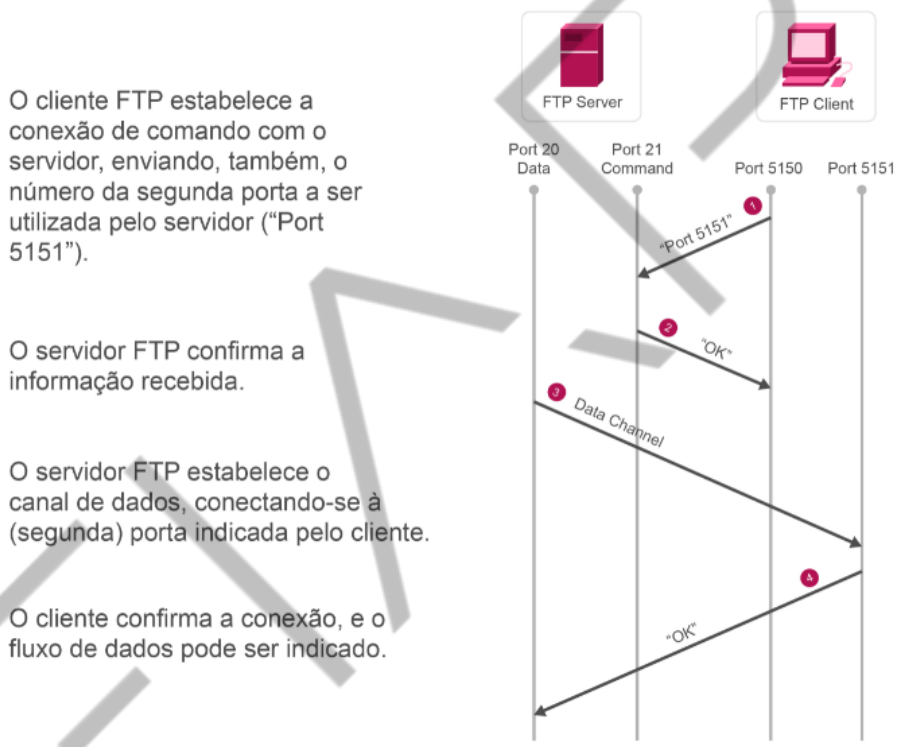

Figura 5.5 – FTP operando em modo ativo
Fonte: Adaptado de CISCO.com (2018)

5.2.2.2 O protocolo FTP em modo passivo

Já no modo passivo, o modelo cliente-servidor é preservado e a *well-known port* 20 não será utilizada, uma vez que, nesse modelo, o cliente originará a conexão referente ao canal de dados a partir de uma porta desprivilegiada em seu *host*, com destino a outra porta desprivilegiada no servidor.

A Figura “FTP operando em modo passivo” ilustra a negociação do protocolo FTP para estabelecimento dos canais de comando e transferência de dados em modo passivo.

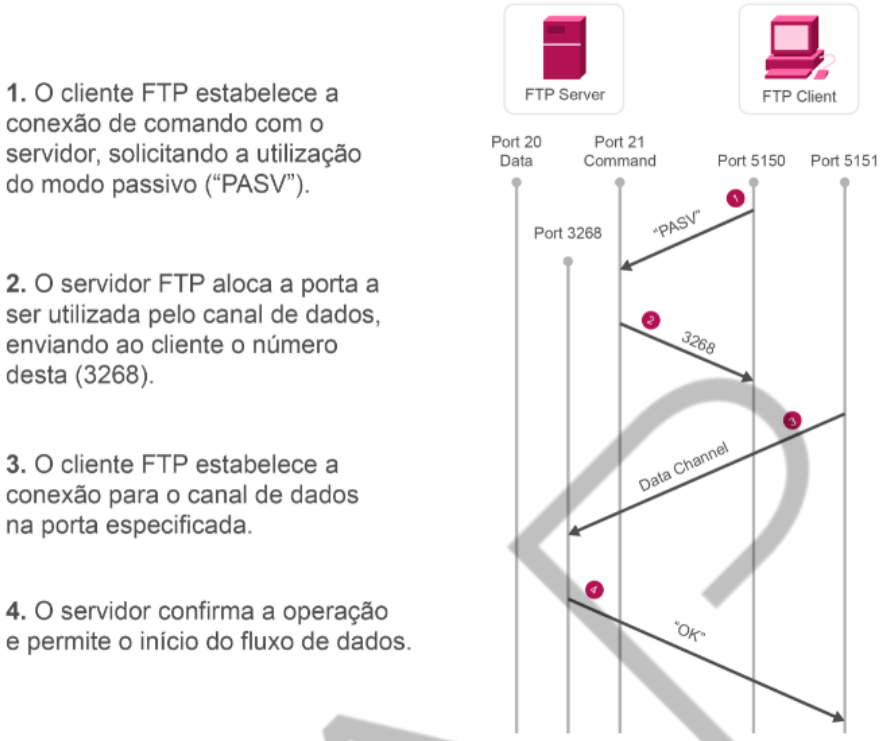

Figura 5.6 – FTP operando em modo passivo
Fonte: Adaptado de CISCO.com (2018)

Independentemente do modo de operação do serviço (ativo ou passivo), observa-se pelo tráfego capturado da sessão FTP representada pela Figura “Captura de sessão FTP” que, dentre outras informações, foi possível obter as credenciais utilizadas pelo usuário para acesso ao serviço, cabendo destacar, ainda, a possibilidade de também obter cópias dos arquivos trafegados na sessão.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.0.0.1	TCP	74	51722 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=393937
2	0.000536	10.0.0.1	10.0.0.2	TCP	74	21 → 51722 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSv
3	0.001405	10.0.0.2	10.0.0.1	TCP	66	51722 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=393937 TSecr=18650
4	0.003269	10.0.0.1	10.0.0.2	FTP	86	Response: 220 (vsFTPd 2.3.4)
5	0.003990	10.0.0.2	10.0.0.1	TCP	66	51722 → 21 [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=393938 TSecr=18650
6	4.453140	10.0.0.2	10.0.0.1	FTP	82	Request: USER anonymous
7	4.453916	10.0.0.1	10.0.0.2	TCP	66	21 → 51722 [ACK] Seq=21 Ack=17 Win=5824 Len=0 TSval=19095 TSecr=395050
8	4.454109	10.0.0.1	10.0.0.2	FTP	100	Response: 331 Please specify the password.
9	4.454791	10.0.0.2	10.0.0.1	TCP	66	51722 → 21 [ACK] Seq=17 Ack=55 Win=29312 Len=0 TSval=395050 TSecr=19095
10	9.885454	10.0.0.2	10.0.0.1	FTP	82	Request: PASS anonymous
11	9.887719	10.0.0.1	10.0.0.2	FTP	89	Response: 230 Login successful.

Figura 5.7 – Captura de sessão FTP
Fonte: Elaborado pelo autor (2020)

Ainda pela Figura “Captura de sessão FTP” é possível observar que – a exemplo do verificado quando da abordagem do protocolo HTTP – também o protocolo FTP depende do TCP para que as conexões necessárias à sua operação sejam estabelecidas.

5.2.3 O protocolo DNS (Domain Name System)

Certamente, o DNS é um dos protocolos de maior relevância para a segurança da informação na medida em que, caso esse serviço venha a ser descontinuado ou subvertido, o impacto sobre o negócio poderá ser bastante relevante.

Resumidamente, o DNS é um banco de dados hierárquico e distribuído, cujo principal objetivo recai sobre a resolução de nomes de domínio, e assim sendo, sua indisponibilidade poderá impactar severamente as operações da rede e o negócio, podendo inviabilizar, durante o período em que se mantiver off-line, a utilização de serviços relacionados à internet, como, por exemplo, a navegação e o envio/recebimento de e-mails.

Não obstante, a quebra da integridade de seus registros, condição algumas vezes referenciada como DNS *cache poisining* (envenenamento do cache DNS), poderia também favorecer a prática de diferentes modalidades de fraudes, como, por exemplo, o direcionando do usuário a uma falsificação do site desejado, a fim de obter ilicitamente informações relevantes, tais como número de suas contas e senhas bancárias.

O DNS também tem dois modos de operação distintos: (a) *lookup*, ou simplesmente resolução de nomes; e (b) *zone transfer*, ou transferência de zona. Basicamente, o *lookup* consiste do mapeamento de um nome de domínio para o respectivo endereço IP e vice-versa, enquanto a *zone transfer* pode ser resumidamente definida como a transferência dos registros de uma zona a outros servidores, geralmente ocorrendo do servidor DNS primário (servidor que controla e armazena os registros da zona sobre a qual tem autoridade) para o servidor DNS secundário (aquele que transfere os registros de zona de outro servidor, primário ou secundário) (Forouzan, 2008).

O serviço DNS opera por padrão na porta 53, utilizando-se, entretanto, como protocolo de transporte o UDP para *lookup* e o TCP para *zone transfer*, uma vez que esse procedimento exige grande confiabilidade. A Tabela “Registros DNS” descreve alguns dos registros DNS mais comumente utilizados.

Tabela 5.1 – Registros DNS

Tipo de registro	Descrição
A (Address)	Retorna o endereço IPv4 mapeado para o domínio especificado, analogamente, o registro AAAA retorna o endereço IPv6 mapeado para o domínio especificado.
	Exemplo: **debian.org. IN A 130.89.148.14**
NS (Name Server)	Retorna os nomes dos servidores (de resolução) de nomes para o domínio especificado.
	Exemplo: **debian.org. IN NS sec1.rcode0.net.**
MX (Mail eXchanger)	Retorna os nomes dos servidores de *e-mails* para o domínio especificado.
	Exemplo: **debian.org. IN MX 0 muffat.debian.org.**
CNAME (Canonical NAME)	Retorna o *alias* (apelido) vinculado ao verdadeiro nome de domínio do *host*.
	Exemplo: **mail.redhat.com. IN CNAME redirect.redhat.com. redirect.redhat.com. IN A 209.132.183.105**
PTR (pointer)	Utilizado para resolução reversa, ou seja, retorna o nome de domínio mapeado para o endereço IP especificado.
	Exemplo: **105.183.132.209.in-addr.arpa. 3352 IN PTR redhat.com.**
TXT (text)	Permite associar um pequeno texto ao *hostname*, a fim de possibilitar a implementação do SPF e o combate ao *spam*.
	Exemplo: **"v=spf1 +a +mx +ip4:65.254.41.45 ?all"**

Fonte: Elaborado pelo autor (2020)

A Figura “Consultas DNS com o dig” ilustra consultas a diferentes registros DNS, realizadas com a ferramenta **dig**, do Linux.

```
user1@target:~$ dig A debian.org +noall +answer

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> A debian.org +noall +answer
;; global options: +cmd
debian.org.             300     IN      A       128.31.0.62
debian.org.             300     IN      A       130.89.148.14
debian.org.             300     IN      A       149.20.4.15
debian.org.             300     IN      A       5.153.231.4
user1@target:~$
user1@target:~$ dig NS debian.org +noall +answer

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> NS debian.org +noall +answer
;; global options: +cmd
debian.org.             28800   IN      NS      sec1.rcode0.net.
debian.org.             28800   IN      NS      sec2.rcode0.net.
debian.org.             28800   IN      NS      dnsnode.debian.org.
user1@target:~$
user1@target:~$ dig MX debian.org +noall +answer

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> MX debian.org +noall +answer
;; global options: +cmd
debian.org.             28800   IN      MX      0 mailly.debian.org.
debian.org.             28800   IN      MX      0 muffat.debian.org.
```

Figura 5.8 – Consultas DNS com o dig
Fonte: Elaborado pelo autor (2020)

A primeira consulta na Figura “Consultas DNS com o dig” solicita os endereços IPv4 (registro A) referentes ao domínio debian.org, enquanto as consultas subsequentes solicitam, respectivamente, os servidores (de resolução) de nomes (registro NS) e servidores de e-mails (registro MX) do referido domínio.

5.2.4 O protocolo SMTP (Simple Mail Transfer Protocol)

O protocolo SMTP é um dos grandes responsáveis pelo fluxo de e-mails na internet. Por padrão, o SMTP trabalha com *plain text*, utilizando o TCP como protocolo de transporte, e ouvindo as requisições na porta 25. Entretanto, a fim de combater a prática de *spam*, o CGI.br (Comitê Gestor da Internet no Brasil) determinou em 2009 que os mecanismos de submissão de mensagens passassem a implementar mecanismos de autenticação e, ainda, que redes de usuários finais de caráter residencial e/ou com endereçamento IP dinâmico tivessem o tráfego de saída bloqueado para a porta 25/TCP, passando-se então a utilizar a porta 465 para conexões criptografadas, embora no Brasil os provedores utilizem, predominantemente, a porta 587.

Basicamente, o SMTP é utilizado quando da necessidade de encaminhamento da mensagem de um usuário a outro, em domínios diferentes; ou ainda, quando a mensagem de um usuário tem múltiplos destinatários, processos que definem o chamado SMTP Relay (relé SMTP).

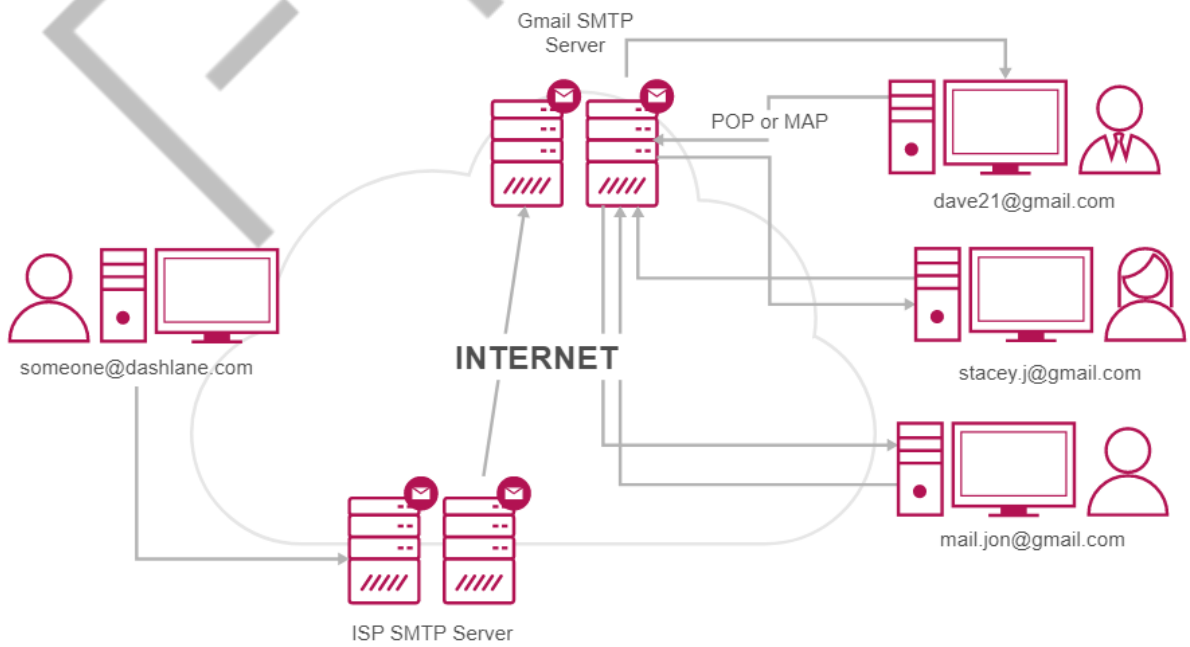

Figura 5.9 – Processo de *relay* do SMTP
Fonte: Adaptado de mailjet.com (2017)

Da Figura “Processo de relay do SMTP” é possível observar que o usuário envia a mensagem ao servidor SMTP de seu provedor, o qual, por sua vez, a repassa ao servidor SMTP do domínio de destino para que seja então entregue aos usuários finais.

Um servidor é classificado como relé aberto (*open relay*) quando processa mensagens de remetentes que não são usuários legítimos de seus serviços, sendo muito utilizado por *spammers* para o envio indiscriminado de e-mails, problema que pode ser mitigado pelo uso do SPF.

5.2.5 O protocolo POP3 (Post Office Protocol v.3)

O protocolo POP3 é um protocolo off-line concebido para acesso remoto à *mailbox* (caixa de correio) onde são armazenadas as mensagens recebidas pelo usuário, possibilitando a ele o *download* dessas mensagens para um computador local.

Originalmente, a exemplo do SMTP, também o POP3 utiliza *plain text*, ouvindo na porta 110/TCP, entretanto, por motivos de segurança, recomenda-se a utilização da porta 995/TCP, a qual permite conexão criptografada por meio do SSL.

5.2.6 Os protocolos Telnet e SSH (Secure Shell)

O Telnet é um protocolo criado na década de 1970, portanto, anterior à própria internet, e possibilita o acesso remoto, via terminal, a recursos como roteadores e switches, dentre outros, possibilitando, ainda, o acesso remoto aos serviços disponibilizados por outros protocolos de camada 7 (modelo OSI), como, por exemplo, o SMTP, POP3 e FTP.

As especificações do Telnet não contemplam autenticação, uma vez que ele é totalmente independente das aplicações que venham a utilizá-lo. Cabe destacar que também o Telnet é baseado em *plain-text*, sendo, portanto, incapaz de garantir a confidencialidade dos dados que transporta, utilizando-se, por padrão, a porta 23/TCP. Simplificadamente, o SSH pode ser descrito como um protocolo alternativo ao Telnet, altamente seguro em decorrência do uso de criptografia (RSA / DSA), operando na porta 22/TCP.

Enquanto o Telnet é comum à maioria dos sistemas operacionais mais populares (mais especificamente: Linux e Windows), o SSH é nativo apenas dos sistemas operacionais UNIX-LIKE, ou seja, sistemas operacionais UNIX e derivados, como, por exemplo, o Linux. Entretanto, o Windows também pode utilizar-se do SSH por meio de aplicações externas, como o **putty**, um emulador de terminal bastante conhecido, muito leve e gratuito, escrito especificamente para essa plataforma; o qual tem conta ainda com o SCP (*secure copy*) e SFTP (*secure file transfer protocol*) para manipulação segura de arquivos.

5.2.7 O protocolo SMB (Server Message Block)

O SMB é o protocolo utilizado pela Microsoft para compartilhamento de arquivos e impressoras em redes Windows. No Windows Server 2019, o protocolo SMB está em sua versão 3, e de acordo com a Microsoft, dentre outras melhorias, destaca-se aqui a criptografia ponta a ponta, dessa maneira evitando a intercepção do tráfego em redes não confiáveis, sem a necessidade de uso do IPSec. Além disso, com o novo recurso há a capacidade de exigir write-through (gravação) em disco em compartilhamentos de arquivos que não estão continuamente disponíveis. Para fornecer uma garantia adicional de que as gravações em um compartilhamento de arquivo percorram toda a pilha de software e hardware até o disco físico antes da operação de gravação retornar como concluída, a Microsoft recomenda que seja habilitado o write-through no compartilhamento de arquivo.

As distribuições Linux implementam o SMB por intermédio do servidor SAMBA, e assim conseguem integrar-se perfeitamente às redes Windows. Cabe reforçar, entretanto, que a versão 1 do protocolo SMB é extremamente vulnerável, e utilizada pelo WannaCry para atacar os sistemas dos usuários, devendo, portanto, ser desabilitada.

A Microsoft fornece as seguintes informações em relação ao SMB:

Tabela 5.2 – Portas do protocolo SMB

Protocolo de aplicativo	Protocolo	Portas
Serviço de datagrama NetBIOS	UDP	138
Resolução de Nomes NetBIOS	UDP	137
Serviço de Sessão NetBIOS	TCP	139
SMB	TCP	445

Fonte: Microsoft (2020)

A partir da Tabela “Portas do protocolo SMB” observa-se que o protocolo SMB utiliza apenas a porta 445/TCP, entretanto, versões mais antigas do Windows (anteriores ao Windows 2000) também podem precisar do protocolo NetBIOS, eventualmente fazendo-se necessário, em decorrência disso, manter-se também estas portas (137,138,139) habilitadas para compatibilidade retroativa.

A Figura “Varredura de portas de host Windows” exibe o resultado de uma varredura de portas feita por meio do **nmap** contra um host Windows, em que é possível observar a porta 445/TCP aberta (indicando que o serviço SMB está ativo), sendo notório, ainda, estar também a porta 139/TCP habilitada.

```
user1@target:~$ nmap -F 192.168.33.10

Starting Nmap 6.47 ( http://nmap.org ) at 2017-11-21 18:16 BRST
Nmap scan report for DESKTOP-G20ICSD (192.168.33.10)
Host is up (0.0026s latency).
Not shown: 96 closed ports
PORT    STATE    SERVICE
135/tcp  filtered  msrpc
139/tcp  filtered  netbios-ssn
445/tcp  filtered  microsoft-ds
```

Figura 5.10 – Varredura de portas de *host* Windows
Fonte: Elaborado pelo autor (2020)

5.2.8 O protocolo NFS (Network File System)

O NFS é um protocolo desenvolvido para possibilitar a montagem de sistemas de arquivos remotos no host local. É o equivalente, no mundo Linux, ao protocolo SMB, tendo, como esse, o objetivo de compartilhar arquivos e diretórios.

Inicialmente desenvolvido pela Sun Microsystems, é totalmente compatível com sistemas Unix/Linux, mas não (diretamente) com sistemas Windows. A implementação do serviço utiliza a porta 2049/TCP-UDP para o protocolo NFS, mais a porta 111/TCP-UDP para o RPCBIND.

5.2.9 O protocolo NTP (Network Time Protocol)

O NTP é um protocolo que obedece a uma topologia hierárquica, criado para sincronização dos relógios dos hosts em redes de dados com latência variável. Por padrão, o NTP trabalha na porta 123/UDP, e apesar de eventualmente parecer um pouco trivial, é um protocolo altamente relevante na medida em que, dentre outros aspectos, o agendamento de tarefas poderá acontecer inoportunamente em função do horário registrado pelos relógios dos hosts, certificados criptográficos e licenças de software poderão expirar inesperadamente e, ainda, *logs* e outras trilhas de auditoria altamente relevantes à segurança da informação poderão perder a integridade.

Outro aspecto também altamente relevante em relação ao NTP diz respeito ao uso dos algoritmos criptográficos que apoiam o serviço, porém, não no sentido de garantir a confidencialidade da informação (no caso, o horário), mas sim no sentido de garantir ao cliente NTP que essa informação é autêntica, ou seja, realmente proveniente dos servidores NTP designados para a rede.

5.3 Tabela resumo

A Tabela “Características básicas dos protocolos” oferece uma visão resumida dos assuntos anteriormente discutidos, oferecendo uma visualização rápida das principais características de cada protocolo.

Tabela 5.3 – Características básicas dos protocolos

Serviço	Protocolo		Porta	Elementos que podem tornar o serviço vulnerável
	L7	L4		
Troca de arquivos, predominantemente, na Internet	FTP	TCP	21	Autenticação fraca, pode quebrar o modelo cliente-servidor, *plain text*
Acesso remoto	TELNET	TCP	23	Desprovido de autenticação própria, *plain text*
Envio de *e-mails*	SMTP	TCP	25	Autenticação fraca, *plain text*
Sistema de nomes de domínio	DNS	TCP/UDP	53	Configuração inadequada ou versões ultrapassadas
Hipertexto (navegação web)	HTTP	TCP	80	*Plain text*, métodos inseguros (GET)
Recebimento de *e-mails*	POP3	TCP	110	Autenticação fraca, *plain text*
Sincronismo dos relógios dos hosts da rede	NTP	UDP	123	Configuração inadequada ou versão ultrapassada
Compartilhamento de arquivos (Windows)	SMB	TCP	445	Configuração inadequada, por exemplo, sem habilitar o uso de criptografia,ou versões ultrapassadas
Compartilhamento de arquivos (Linux)	NFS RPCBIND	TCP/UDP UDP		

Fonte: Elaborado pelo autor (2020)

5.4 testando um servidor smtp

5.4.1 Utilizando Telnet para teste do serviço SMTP

Este procedimento utiliza o Telnet para testes básicos de um servidor SMTP, tendo-se como referência o cenário representado pela Figura “Cenário simplificado”.

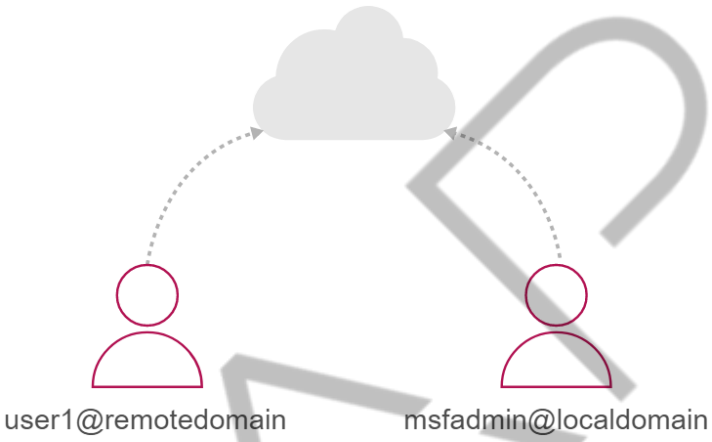

Figura 5.11 – Cenário simplificado
Fonte: Elaborado pelo autor (2020)

Sessão Telnet de user1@remotedomain, originada remotamente:

```
root@host-1:/#telnet 10.0.0.1 25 [1]
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
helo remotedomain [2]
250 metasploitable.localdomain [3]
250 2.1.0 Ok
rcpt to: msfadmin@localhost [4]
250 2.1.5 Ok
data [5]
354 End data with <CR><LF>.<CR><LF>
Texto enviado com a mensagem
from: user1@remotedomain
to: msfadmin@localhost
Esta e a mensagem enviada a partir de um usuario remoto (user1) a um usuario
local (msfadmin)
. [6]
250 2.0.0 Ok: queued as E6952CCA4
quit [7]
221 2.0.0 Bye
Connection closed by foreign host.
root@host-1:/#
```

Figura 5.12 – Comandos da sessão Telnet
Fonte: Elaborado pelo autor (2020)

Da Figura “Comandos da sessão Telnet” é possível observar que a sessão é aberta pelo usuário remoto por meio do Telnet, indicando ao final da linha de comando do cliente Telnet, a porta 25 como destino **[1]**. Por sua vez, o servidor, sem solicitar autenticação desse usuário, aceita o início da sessão, e o usuário remoto identifica seu domínio como remetente da mensagem **[2]**. As linhas **[3]** e **[4]** indicam respectivamente o remetente e o destinatário da mensagem. O comando data **[5]** possibilita a entrada do conteúdo da mensagem a ser enviada, ressaltando-se aqui a necessidade de digitação de um ponto final **[6]** para indicar que a digitação já foi finalizada, e que, portanto, a mensagem deve ser enviada. A sessão é então finalizada pelo quit **[7]**.

A Figura “Mensagem final enviada” mostra a mensagem final enviada ao destinatário.

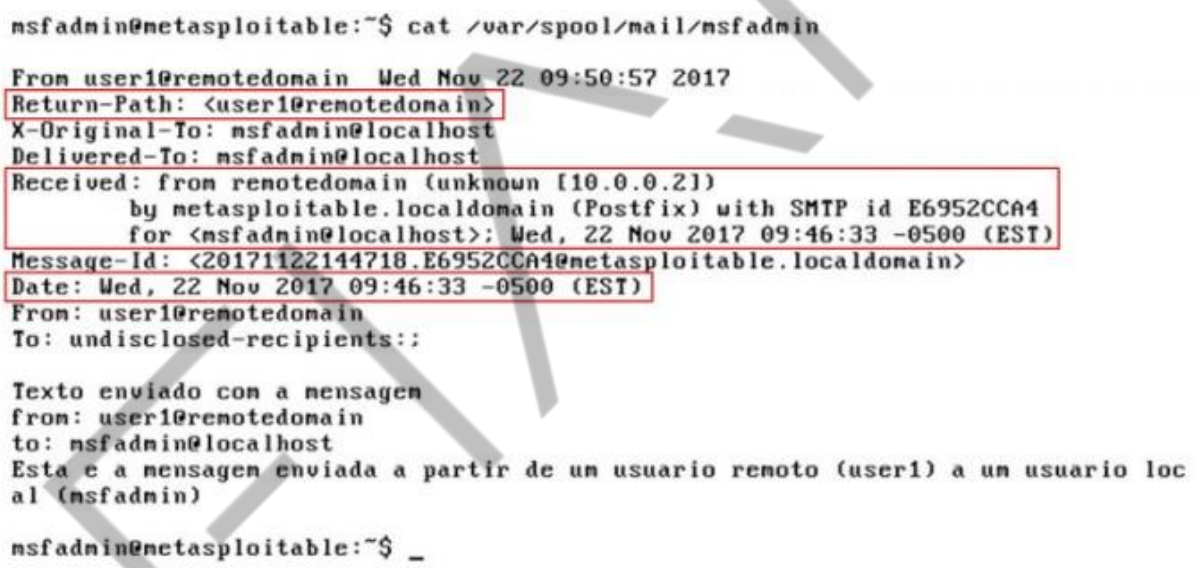

Figura 5.13 – Mensagem final enviada
Fonte: Elaborado pelo autor (2020)

Observa-se pela Figura “Mensagem final enviada” que o arquivo /var/spool/mai/**msfadmin** é a caixa postal, no servidor SMTP, onde a mensagem foi armazenada. Pelo primeiro destaque é possível observar que as mensagens de retorno deverão ser enviadas ao e-mail especificado no campo Return-Path (user1@remotedomain), verificando-se na sequência que o domínio de origem da mensagem é *remotedomain*, tendo o *host* remetente da mensagem o endereço IP 10.0.0.2 (de onde pode-se presumir que o envio foi feito por um *host* na mesma rede em que reside o servidor), tendo-se abaixo o *timestamp* e o conteúdo da mensagem.

REFERÊNCIAS

BLANK, A. G. **TCP/IP Foundations**. Alameda: Sybex Inc., 2004.

FARREL, A. **A Internet e seus protocolos. Uma análise comparativa**. Rio de Janeiro: Elsevier, 2005.

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 4. ed. São Paulo: McGraw-Hill, 2008.

HUNT, C. **TCP/IP Network Administration.** 3. ed. Sebastopol: O'Reilly Media, 2010.

IANA. **Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry**. Disponível em: <https://tools.ietf.org/html/rfc6335#page-16>. Acesso em: 21 abr. 2020.

IANA. **Service Name and Transport Protocol Port Number Registry**. Disponível em: <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>. Acesso em: 21 abr. 2020.

PETERSON, L. L.; DAVIE, R. S. **Redes de Computadores – Uma abordagem de sistemas**. 3. ed. Rio de Janeiro: Elsevier, 2004.

_____. **Registros de Recursos de DNS**. 2006. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ip/domain-name-system-dns/12684-dns-resource.html>. Acesso em: 21 abr. 2020.

_____. **Resolução CGI.br/RES/2009/002/P**. 2009. Disponível em: <https://www.cgi.br/resolucoes/documento/2009/CGI.br_Resolucao_2009_002.pdf>. Acesso em: 21 abr. 2020.

GLOSSÁRIO

Extranet	Pode ser simplificadamente definida como um segmento de rede que possibilita o compartilhamento de recursos com usuários externos, de forma controlada. Pode ser de grande valor para o negócio, promovendo maior integração e agilidade nas operações da empresa com clientes e colaboradores em geral.
Serviços de diretório	Os serviços de diretório consistem de softwares que armazenam e organizam as informações de grupos de usuários, possibilitando aos administradores gerenciarem o acesso desses usuários aos sistemas e recursos computacionais.
Plain Text	Formato de texto simples (puro) e sem formatação, tornando-se em decorrência disso a forma mais eficiente para armazenamento de texto. Suporta caracteres ASCII, incluindo números, símbolos e espaços.
Spam	São e-mails não solicitados, geralmente enviados para um grande número de destinatários.
SPF	Tecnologia para combate à falsificação do *return-path* (endereço de retorno) dos e-mails. Permite ao administrador de um domínio definir os endereços dos servidores autorizados a enviar mensagens em nome desse domínio, permitindo também aos administradores de serviços de e-mail estabelecer os critérios para a aceitação dessas mensagens em função das políticas SPF de cada domínio. Leia mais em: <http://www.antispam.br/admin/spf/>.