Laboratório 4.5.3: Análise de Protocolos das Camadas de Aplicação e Transporte

Diagrama de Topologia

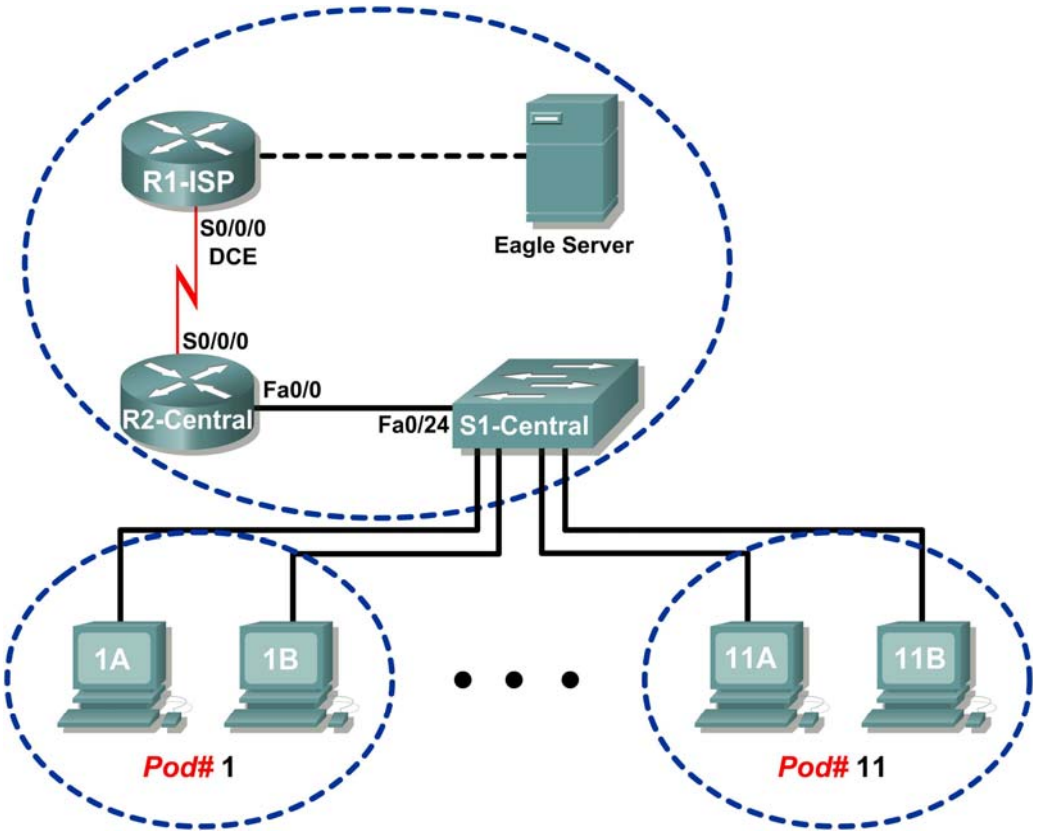


Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway Padrão
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*N/A*
	Fa0/0	192.168.254.253	255.255.255.0	*N/A*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*N/A*
	Fa0/0	172.16.255.254	255.255.0.0	*N/A*
Eagle Server	*N/A*	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	*N/A*
host*Pod#*A	*N/A*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	*N/A*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*N/A*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos

Com a conclusão deste laboratório, você será capaz de:

- Configurar o computador para capturar protocolos de camada de Aplicação.
- Capturar e analisar comunicação HTTP entre o computador e um servidor web.
- Capturar e analisar comunicação FTP entre o computador e um servidor FTP.
- Observar o TCP estabelecer e gerenciar canais de comunicação com as conexões HTTP e FTP.

Contexto

A função principal da Camada de Transporte é manter registro de múltiplas conversas de aplicação no mesmo host. No entanto, aplicações diferentes possuem exigências diferentes para seus dados e, portanto, diferentes protocolos de Transporte foram desenvolvidos para atender essas exigências. Protocolos da camada de Aplicação definem a comunicação entre os serviços de rede, tais como um servidor web e um cliente, e um servidor FTP e um cliente. Os clientes iniciam a comunicação ao servidor adequado, e o servidor responde ao cliente. Para cada serviço de rede existe um servidor diferente ouvindo uma porta diferente para conexões de clientes. Podem existir vários servidores no mesmo dispositivo final. Um usuário pode abrir várias aplicações de clientes no mesmo servidor, ainda cada cliente se comunica exclusivamente com uma sessão estabelecida entre o cliente e o servidor.

Protocolos da camada de Aplicação contam com protocolos TCP/IP de camada inferior, tais como TCP ou UDP. Este laboratório irá examinar dois protocolos populares da Camada de Aplicação, o HTTP e o FTP, e como os protocolos TCP e UDP da Camada de Transporte gerenciam o canal de comunicação. Também serão examinadas as solicitações comuns de cliente e as correspondentes respostas do servidor.

Cenário

Neste laboratório, você irá usar aplicações de cliente para se conectar aos serviços de rede do eagle-server. Você irá monitorar a comunicação com o Wireshark e analisar os pacotes capturados.

Um navegador como o Internet Explorer ou o Firefox será usado para se conectar ao serviço de rede do eagle-server. O eagle-server possui vários serviços de rede pré-configurados, tais como o HTTP, esperando para responder solicitações de clientes.

O navegador também será usado para examinar o protocolo FTP, bem como o cliente de linha de comando FTP. Este exercício demonstrará que embora os clientes possam diferir a comunicação básica ao servidor, este permanece o mesmo.

Tarefa 1: Configurando o Computador para Capturar Protocolos da Camada de Aplicação

O laboratório deve estar configurado como mostra o Diagrama de Topologia e a tabela de endereço lógico. Caso não esteja, peça auxílio ao instrutor antes de prosseguir.

Se um computador individual não conseguir se conectar ao eagle-server, verifique a conexão de cabos entre o host e S1-Central. Verifique se o computador possui o endereço IP correto, exibido na tabela de endereçamento lógico acima, e se ele consegue fazer ping em R2-Central.

Passo 1: Fazer o Download e Instalar o Wireshark.

Figura 1. Download FTP para Wireshark

Se o Wireshark não estiver instalado no computador, você pode fazer o download do eagle-server.example.com. Veja a Figura 1. A URL para download é ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3.

1. Clique com o botão direito do mouse no nome do arquivo do Wireshark e salve o arquivo no computador.
2. Quando o download do arquivo estiver completo, dê duplo clique no nome do arquivo e instale o Wireshark com as configurações padrão.

Passo 2: Iniciar o Wireshark e configurar a Interface de Captura.

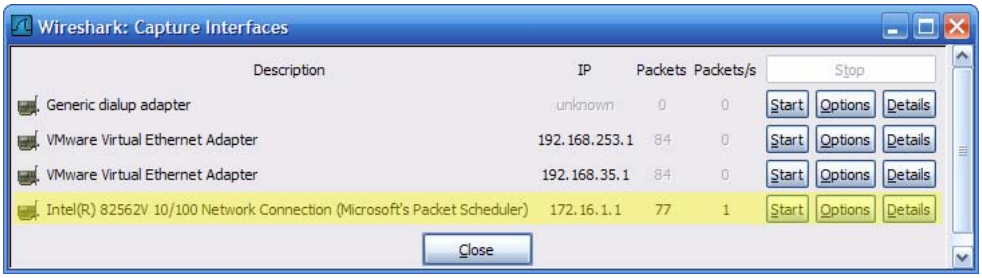
1. Inicie o Wireshark em **Iniciar > Todos os Programas > Wireshark > Wireshark**.
2. Quando a tela inicial aparecer, configure a Interface de Captura correta. A interface com o endereço IP do computador é a interface correta. Veja a Figura 2.
3. 

Figura 2. Tela de Captura de Interface do Wireshark

O Wireshark pode ser iniciado clicando no botão **Iniciar** da interface. Posteriormente, a interface é usada como a padrão e não precisa ser alterada.

O Wireshark deve começar a registrar dados.

4. Pare o Wireshark por um momento. O Wireshark será usado em tarefas posteriores.

Tarefa 2: Capturando e Analisando Comunicação HTTP Entre o Computador e um Servidor Web

O HTTP é um protocolo da camada de Aplicação, contando com protocolos de nível inferior como o TCP para estabelecer e gerenciar o canal de comunicação. A versão 1.1 do HTTP é definida no RFC 2616, com data de 1999. Esta parte do laboratório demonstrará como as sessões entre múltiplos clientes web e o servidor web são mantidas separadas.

Passo 1: Iniciar as capturas do Wireshark.

Inicie uma captura do Wireshark. O Wireshark exibirá capturas baseadas no tipo de pacote.

Passo 2: Iniciar o navegador.

1. Usando um navegador como o Internet Explorer ou o Firefox, conecte-se à URL http://eagle-server.example.com. Uma página web similar à Figura 3 será exibida. Não feche este navegador até que instruído a fazê-lo.

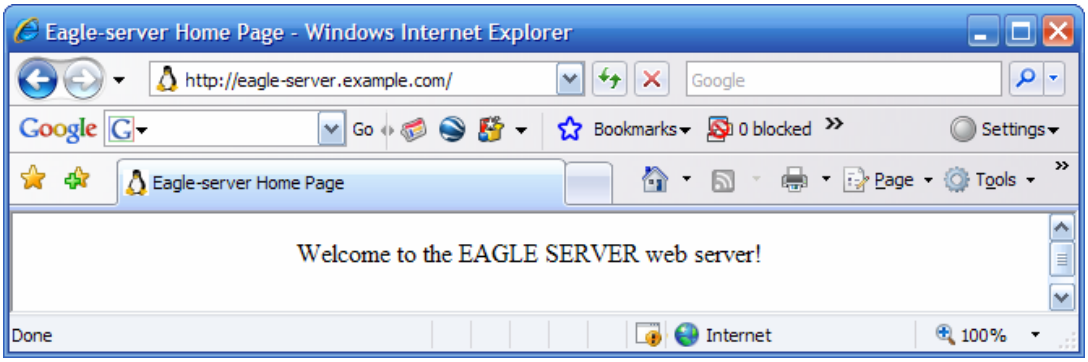


Figura 3. Navegador Conectado ao Servidor Web

2. Clique no botão **Renovar** do navegador. Não deve haver alteração à exibição no cliente web.
3. Abra um segundo navegador e se conecte à URL http://eagle-server.example.com/page2.html. Isso exibirá uma página web diferente.

   Não feche nenhum dos navegadores até que seja concluída a captura do Wireshark.

Passo 3: Parar as capturas do Wireshark e analisar os dados capturados.

1. Pare as capturas do Wireshark.
2. Feche os navegadores.

Os dados do Wireshark resultantes serão exibidos. Havia na verdade pelo menos três sessões HTTP criadas no Passo 2. A primeira sessão HTTP iniciou com uma conexão ao http://eagle-server.example.com. A segunda sessão ocorreu com uma ação de atualização. A terceira sessão ocorreu quando o segundo navegador acessou http://eagle-server.example.com/page2.html.

No.	Time	Source	Destination	Protocol	Info
10	10.168217	172.16.1.2	192.168.254.254	TCP	1056 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.170734	192.168.254.254	172.16.1.2	TCP	http > 1056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
12	10.170767	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	10.171086	172.16.1.2	192.168.254.254	HTTP	GET / HTTP/1.1
14	10.171625	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=1 Ack=208 Win=6432 Len=0
15	10.172518	192.168.254.254	172.16.1.2	HTTP	HTTP/1.1 200 OK (text/html)
16	10.172540	192.168.254.254	172.16.1.2	TCP	http > 1056 [FIN, ACK] Seq=448 Ack=208 Win=6432 Len=0
17	10.172567	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=208 Ack=449 Win=63793 Len=0
18	10.174196	172.16.1.2	192.168.254.254	TCP	1056 > http [FIN, ACK] Seq=208 Ack=449 Win=63793 Len=0
19	10.174661	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=449 Ack=209 Win=6432 Len=0

Figura 4. Sessão HTTP Capturada

Uma sessão HTTP capturada como amostra é exibida na Figura 4. Antes do HTTP ter início, a sessão TCP deve ser criada. Isso é visto nas primeiras três linhas de sessão, números 10, 11 e 12. Use sua captura ou saída do Wireshark similar para responder as seguintes perguntas:

3. Preencha a tabela a seguir das informações apresentadas na sessão HTTP:

Endereço IP do navegador	
Endereço IP do servidor web	
Protocolo de camada de transporte (UDP/TCP)	
Número de porta do navegador	
Número de porta do servidor web	

4. Qual computador iniciou a sessão HTTP, e como?

_____

_____

5. Qual computador inicialmente sinalizou o final da sessão HTTP, e como?

_____

_____

6. Destaque a primeira linha do protocolo HTTP, uma solicitação **GET** do navegador. Na Figura 4 acima, a solicitação **GET** está na linha 13. Vá para a segunda (do meio) janela do Wireshark para examinar os protocolos em camadas. Se necessário, expanda os campos.
7. Qual protocolo é levado (encapsulado) dentro do segmento TCP?

_____

8. Expanda o último registro de protocolo e quaisquer sub-campos. Esta é a informação real enviada ao servidor web. Complete a tabela a seguir usando informações do protocolo.

Versão do Protocolo	
Método de Solicitação	
* Solicitação URI	
Idioma	

* Solicitação URI é o caminho ao documento solicitado. No primeiro navegador, o caminho é o diretório raiz do servidor web. Embora nenhuma página tenha sido solicitada, alguns servidores web são configurados para exibir um arquivo padrão se um estiver disponível.

O servidor web responde com o próximo pacote HTTP. Na Figura 4, ele está na linha 15. Uma resposta ao navegador é possível porque o servidor web (1) entende o tipo de solicitação e (2) tem um arquivo para retornar. Crackers às vezes enviam solicitações desconhecidas ou distorcidas aos servidores web em uma tentativa de parar o servidor ou obter acesso à linha de

comando do servidor. Além disso, uma solicitação para uma página web desconhecida resultará em uma mensagem de erro.

9. Destaque a resposta do servidor web e, então, vá para a segunda janela (do meio). Abra todos os sub-campos de HTTP que sofreram colapso. Note que as informações voltaram do servidor. Nesta resposta, existem somente algumas linhas de texto (respostas de servidor web podem conter milhares ou milhões de bytes). O navegador entende e formata corretamente os dados na janela do navegador. .
10. Qual é a resposta do servidor web à solicitação **GET** do cliente web?

_____

11. O que essa resposta significa?

_____

_____

12. Vá até a janela superior do Wireshark até a segunda sessão HTTP, atualize, é visível. Uma captura de amostra é exibida na Figura 5.

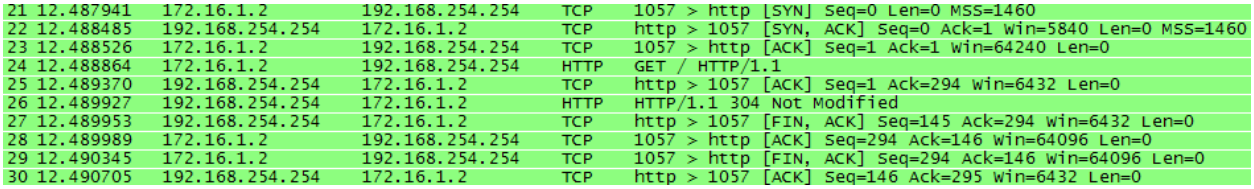


Figura 5. Sessão HTTP Capturada para Renovação

A importância da ação de renovação está na resposta do servidor, **`304 Não Modificado`**. Com um único pacote devolvido tanto para a solicitação **GET** inicial e de atualização, a largura de banda usada é mínima. No entanto, para uma resposta inicial que contenha milhões de bytes, um único pacote de resposta pode não desperdiçar uma largura de banda significativa.

Pelo fato desta página web ter sido salva no cache do cliente web, a solicitação **GET** continha as seguintes instruções adicionais ao servidor web:

```
Se-modificado-desde: Sex, 26 Jan 2007 06:19:33 GMT\r\n
Se-Nenhum-Comparado: “98072-b8-82da8740”\r\n  <- número de tag de página (ETAG)
```

13. Qual é a resposta ETAG do servidor web?

_____

Tarefa 3: Capturando e Analisando Comunicação FTP entre o Computador e um Servidor Web

O protocolo da camada de Aplicação FTP passou por uma revisão significativa desde sua primeira aparição no RFC 114, em 1971. A versão 5.1 do FTP é definida no RFC 959, de outubro de 1985.

O navegador familiar pode ser usado para se comunicar com mais do que somente o servidor HTTP. Nesta tarefa, o navegador e um utilitário FTP de linha de comando serão usados para fazer download de dados de um servidor FTP.

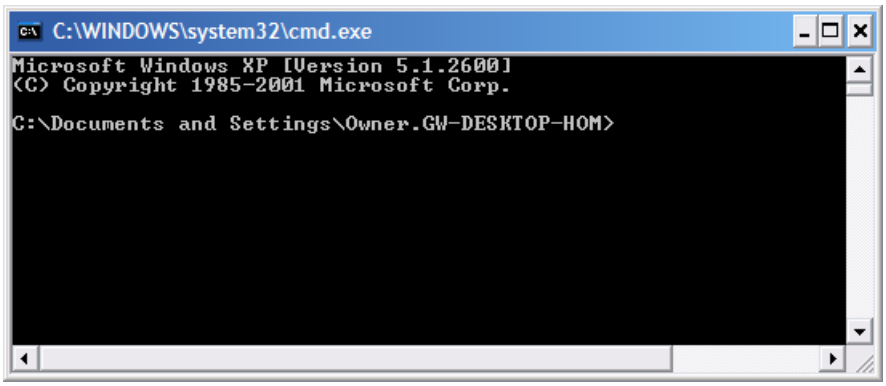


Figura 6. Tela de Linha de Comando Windows

Em preparação para esta tarefa, abra uma linha de comando no computador. Isso pode ser realizado clicando em **Iniciar > Executar**, e então digitando **CMD** e clicando em **OK**. Uma tela similar à Figura 6 será exibida.

Passo 1: Iniciar as capturas do Wireshark.

Se necessário, consulte a Tarefa 1, Passo 2, para abrir o Wireshark.

Passo 2: Iniciar o cliente FTP de linha de comando.

1. Inicie uma sessão FTP do computador com o servidor FTP, usando o utilitário de cliente FTP Windows. Para autenticar, use o ID de usuário **anônimo**. Em resposta ao prompt da senha, pressione <**ENTER**>.

```
>ftp eagle-server.example.com
Conectado a eagle-server.example.com.
220 Bem vindo ao serviço de FTP eagle-server.
Usuário (eagle-server.example.com:(nenhum)): anônimo
331 Por favor, especifique a senha.
Senha: <ENTER>
230 Login com sucesso.
```

2. O prompt do cliente FTP é `ftp>`. Isso significa que o cliente FTP está esperando por um comando para enviar ao servidor FTP. Para visualizar uma lista de comandos de cliente FTP, digite **`help <ENTER>`**:

```
ftp> help
Comandos podem ser abreviados.  Os comandos são:

!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

Infelizmente, o grande número de comandos de cliente FTP faz com que o uso do utilitário de linha de comando seja difícil para novatos. Usaremos somente alguns comandos para avaliação do Wireshark.

3. **Digite o comando `dir` para exibir o conteúdo do diretório atual:**

```
ftp> dir
200 comando de PORTA com sucesso. Considere usando PASV.
150 Aí vem a lista de diretório.
drwxr-xr-x    3 0        0            4096 Jan 12 04:32 pub
```

O cliente FTP está no diretório raiz do servidor FTP. Este não é o diretório raiz real do servidor—somente o ponto mais alto que o usuário **anônimo** consegue acessar. O usuário **anônimo** foi colocado em uma raiz fechada, proibindo o acesso fora do diretório atual.

4. No entanto, sub-diretórios podem ser acessados e arquivos transferidos ao computador. Vá até o diretório pub/eagle_labs/eagle1/chapter2, faça o download de um arquivo e saia.

```
ftp> cd pub/eagle_labs/eagle1/chapter2
250 Diretório alterado com êxito.
ftp> dir
200 comando de PORTA com sucesso. Considere usando PASV.
150 Aí vem a lista de diretório.
-rw-r--r--  1 0 100     5853 Jan 12 04:26 ftptoeagle-server.pcap
-rw-r--r--  1 0 100     4493 Jan 12 04:27 http to eagle-server.pcap
-rw-r--r--  1 0 100     1486 Jan 12 04:27 ping to 192.168.254.254.pcap
-rw-r--r--  1 0 100 15163750 Jan 12 04:30 wireshark-setup-0.99.4.exe
226 Envio de diretório OK.
ftp: 333 bytes recebidos em 0.04Segundos 8.12Kbytes/seg.
ftp> get "ftptoeagle-server.pcap"
200 comando de PORTA com sucesso. Considere usando PASV.
150 Abrindo conexão de dados de modo BINÁRIO para ftptoeagle-server.pcap (5853
bytes).
226 Arquivo enviado OK.
ftp: 5853 bytes recebidos em 0.34Segundos 17.21Kbytes/seg.
ftp> parar
221 Adeus.
```

5. Feche a janela de linha de comando com o comando **exit**.
6. Pare as capturas do Wireshark e salve as capturas como `FTP_Command_Line_Client`.

Passo 3: Iniciar o navegador.

1. Inicie as capturas do Wireshark novamente.

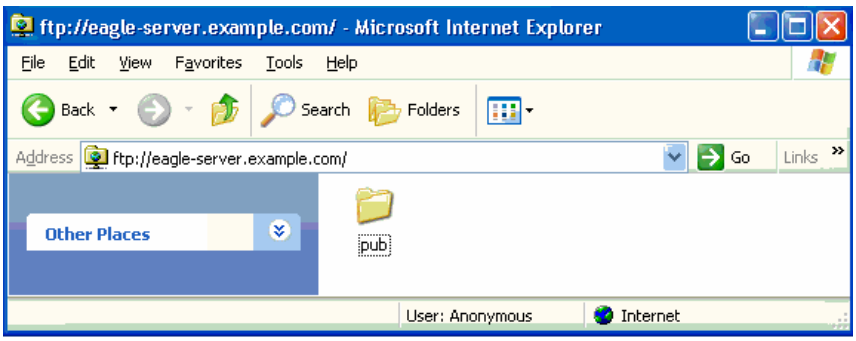


Figura 7. Navegador Usado como um Cliente FTP.

Abra um navegador como mostra a Figura 7 e digite na URL ftp://eagle-server.example.com. Uma janela do navegador é aberta com o diretório pub exibido. Ainda, o navegador está conectado ao servidor FTP com o usuário Anônimo, como mostra na parte inferior da captura de tela.

2. Usando o navegador, desça pelos diretórios até o caminho da URL `pub/eagle-labs/eagle1/chapter2`. Dê duplo clique no arquivo `ftptoeagle-server.pcap` e o salve.
3. Quando terminar, feche o navegador.
4. Pare as capturas do Wireshark e as salve como FTP_Web_Browser_Client.

Passo 4: Parar as capturas do Wireshark e analisar os dados capturados.

1. Se ainda não estiver aberta, abra a captura do Wireshark FTP_Web_Browser_Client.
2. Na parte superior da janela do Wireshark, selecione a captura FTP que é a primeira transmissão de protocolo FTP, Resposta: 220. Na Figura 8, esta é a linha 23.

No.	Time	Source	Destination	Protocol	Info
12	16.276555	172.16.1.2	192.168.254.254	DNS	Standard query A eagle-server.example.com
13	16.277284	192.168.254.254	172.16.1.2	DNS	Standard query response A 192.168.254.254
14	16.278059	172.16.1.2	192.168.254.254	TCP	1073 > ftp [SYN] Seq=0 Len=0 MSS=1460
15	16.278540	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	16.278575	172.16.1.2	192.168.254.254	TCP	1073 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	26.281472	192.168.254.254	172.16.1.2	FTP	Response: 220 Welcome to the eagle-server FTP service.
24	26.281672	172.16.1.2	192.168.254.254	FTP	Request: USER anonymous
25	26.282120	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [ACK] Seq=47 Ack=17 Win=5840 Len=0
26	26.282137	192.168.254.254	172.16.1.2	FTP	Response: 331 Please specify the password.
27	26.282201	172.16.1.2	192.168.254.254	FTP	Request: PASS IEUser@
28	26.283451	192.168.254.254	172.16.1.2	FTP	Response: 230 Login successful.
29	26.313423	172.16.1.2	192.168.254.254	FTP	Request: opts utf8 on
30	26.313959	192.168.254.254	172.16.1.2	FTP	Response: 501 Option not understood.
31	26.314042	172.16.1.2	192.168.254.254	FTP	Request: syst
32	26.314493	192.168.254.254	172.16.1.2	FTP	Response: 215 UNIX Type: L8
33	26.314595	172.16.1.2	192.168.254.254	FTP	Request: site help
34	26.315028	192.168.254.254	172.16.1.2	FTP	Response: 550 Permission denied.
35	26.315113	172.16.1.2	192.168.254.254	FTP	Request: PWD
36	26.315566	192.168.254.254	172.16.1.2	FTP	Response: 257 "/"
37	26.352350	172.16.1.2	192.168.254.254	FTP	Request: noop
38	26.352821	192.168.254.254	172.16.1.2	FTP	Response: 200 NOOP ok.
39	26.482680	172.16.1.2	192.168.254.254	FTP	Request: CWD /
40	26.483243	192.168.254.254	172.16.1.2	FTP	Response: 250 Directory successfully changed.
41	26.484334	172.16.1.2	192.168.254.254	FTP	Request: TYPE A
42	26.484824	192.168.254.254	172.16.1.2	FTP	Response: 200 Switching to ASCII mode.
43	26.485292	172.16.1.2	192.168.254.254	FTP	Request: PORT 172,16,1,2,4,50
44	26.485800	192.168.254.254	172.16.1.2	FTP	Response: 200 PORT command successful. Consider using PASV.
45	26.485892	172.16.1.2	192.168.254.254	FTP	Request: LIST
46	26.486503	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [SYN] Seq=0 Len=0 MSS=1460 TSV=12998374 TSER=0 WS=2
47	26.486558	172.16.1.2	192.168.254.254	TCP	1074 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=
48	26.486948	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=12998375 TSER=0
49	26.487052	192.168.254.254	172.16.1.2	FTP	Response: 150 Here comes the directory listing.
50	26.487252	192.168.254.254	172.16.1.2	FTP-DA	FTP Data: 61 bytes
51	26.487267	192.168.254.254	172.16.1.2	FTP	Response: 226 Directory send OK.

Figura 8. Captura Wireshark de uma Sessão FTP com um Navegador

3. Vá até a janela do meio do Wireshark e expanda o protocolo FTP. O FTP se comunica usando códigos, igual ao HTTP.

Qual é a resposta 220 do servidor FTP?

_____

Quando o servidor FTP emitiu uma Resposta: 331 Por favor, especifique a senha, qual foi a resposta do navegador?

_____

Qual número de porta o cliente FTP usa para se conectar à porta 21 do servidor FTP?

_____

Quando os dados são transferidos ou quando listando diretório simples, uma nova porta é aberta. Isso é chamado modo de transferência. O modo de transferência pode ser ativo ou passivo. No modo ativo, o servidor abre uma sessão TCP ao cliente FTP e transfere dados por aquela porta. O número da porta de origem do servidor FTP é 20 e o número de porta do cliente FTP é algum número acima de 1023. No

entanto, no modo passivo, o cliente abre uma nova porta ao servidor para transferência de dados. Ambos os números de porta são acima de 1023.

Qual é o número de porta FTP-DADOS usado pelo servidor FTP?

_____

4. Abra a captura do Wireshark FTP_Web_Browser_Client e observe a comunicação FTP. Embora os clientes sejam diferentes, os comandos são similares.

Passo 5: Modos de transferência ativo e passivo do FTP

As implicações entre os dois modos são bastante importantes de uma perspectiva de segurança de informações. O modo de transferência determina como a porta de dados é configurada.

No modo de transferência ativo, um cliente inicia uma sessão FTP com o servidor na porta 21 TCP conhecida. Para transferência de dados, o servidor inicia uma conexão da porta 20 TCP conhecida a uma porta alta do cliente, um número de porta acima de 1023. Veja a Figura 9.

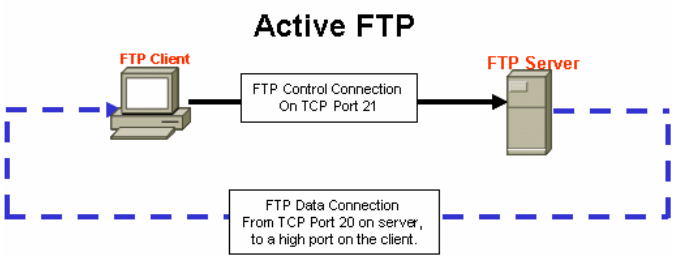


Figura 9.

A menos que o firewall do cliente FTP esteja configurado para permitir conexões externas, a transferência de dados pode falhar. Para estabelecer conectividade para transferência de dados, o cliente FTP deve permitir conexões relacionadas a FTP (implicando filtragem de pacote stateful), ou desabilitar o bloqueio.

No modo de transferência passivo, um cliente inicia uma sessão FTP com o servidor na porta 21 TCP, a mesma conexão usada no modo de transferência ativo. No entanto, para transferência de dados, existem duas alterações significativas. Primeira, o cliente inicia a conexão de dados ao servidor. Segunda, portas altas são usadas em ambas as extremidades da conexão. Veja a Figura 10.

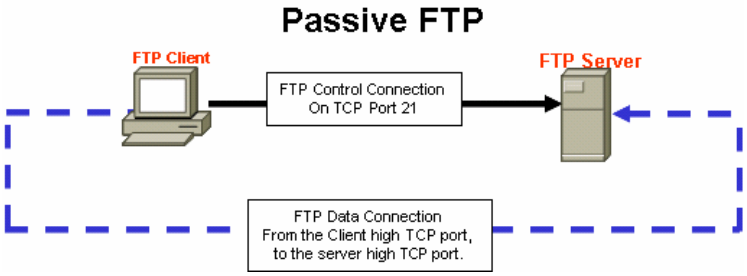


Figura 10.

A menos que o servidor FTP esteja configurado para permitir uma conexão a uma porta alta aleatória, a transferência de dados falhará. Nem todas as aplicações de cliente FTP suportam alterações no modo de transferência.

Tarefa 4: Reflexão

Ambos os protocolos HTTP e FTP contam com o TCP para se comunicar. O TCP gerencia a conexão entre cliente e servidor para garantir a entrega de datagrama.

Uma aplicação de cliente pode ser tanto um navegador quanto um utilitário de linha de comando, mas cada um deles deve enviar e receber mensagens que possam ser interpretadas corretamente. O protocolo de comunicação é normalmente definido em um RFC.

O cliente FTP deve se autenticar ao servidor FTP, mesmo se a autenticação for aberta ao mundo. O usuário Anônimo normalmente restringiu acesso ao servidor FTP e não pode carregar arquivos.

Uma sessão HTTP é iniciada quando uma solicitação é feita ao servidor HTTP e termina quando a resposta foi reconhecida pelo cliente HTTP. Uma sessão FTP, no entanto, dura até o cliente sinalizar que está saindo com o comando **`exit`**.

O HTTP usa um único protocolo para se comunicar com o servidor HTTP. O servidor ouve a porta 80 para conexões de cliente. O FTP, no entanto, usa dois protocolos. O servidor FTP ouve a porta 21 TCP, como a linha de comando. Dependendo do modo de transferência, o servidor ou o cliente poderá iniciar a conexão de dados.

Múltiplos protocolos da camada de Aplicação podem ser acessados através de um navegador simples. Embora somente o HTTP e o FTP tenham sido examinados, o Telnet e o Gopher também podem ser suportados no navegador. O navegador atua como um cliente ao servidor, enviando solicitações e respostas de processamento.

Tarefa 5: Desafio

Habilitando a captura Wireshark, use um navegador para navegar ao R2 em `http://172.16.255.254/level/7/exec` ou use um cliente Telnet para se conectar a um dispositivo Cisco como S1-Central ou R2-Central. Observe o comportamento do protocolo HTTP ou Telnet. Emita alguns comandos para observar os resultados.

Como o protocolo Telnet da camada de Aplicação é similar ao HTTP e ao FTP? Como o TELNET é diferente?

_____

Tarefa 6: Limpeza

Se o Wireshark foi instalado no computador para este laboratório, o instrutor pode querer o aplicativo removido. Para remover o Wireshark, clique em **Iniciar > Painel de Controle > Adicionar ou Remover Programas**. Vá até a parte inferior da lista, clique com o botão direito do mouse em **Wireshark** e clique em **Remover**.

Se arquivos instalados precisam ser removidos do computador, apague-os do servidor FTP.

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.

