Tópicos Especiais em Segurança da Informação

TP3 - Reconhecimento do ponto de vista de um insider (Wireshark)

Arthur do Prado Labaki

24-05, 2022

GBC 235

Informações adicionais

Todas as imagens integradas nesse relatório, quanto códigos, planilhas ou gifs de demonstração estão em meu repositório no github abaixo.
Link do meu GitHub

Parte 1:

Resolução do item 1)

Um analisador de pacotes ou farejador de pacotes (*packet analyzer*) é um software ou hardware que consegue rastrear, interceptar e registrar o tráfego que passa pela rede. Conforme os fluxos de dados fluem pela rede, o analisador captura cada pacote e, se necessário, decodifica os dados brutos do pacote, mostrando os valores de vários campos no pacote e analisa seu conteúdo de acordo com a RFC apropriada ou outras especificações (Nakamura e Geus, 2007). Um analisador de pacotes mostra o status completo de todas as atividades de rede, fornecendo uma imagem completa da largura de banda e da utilização de recursos.

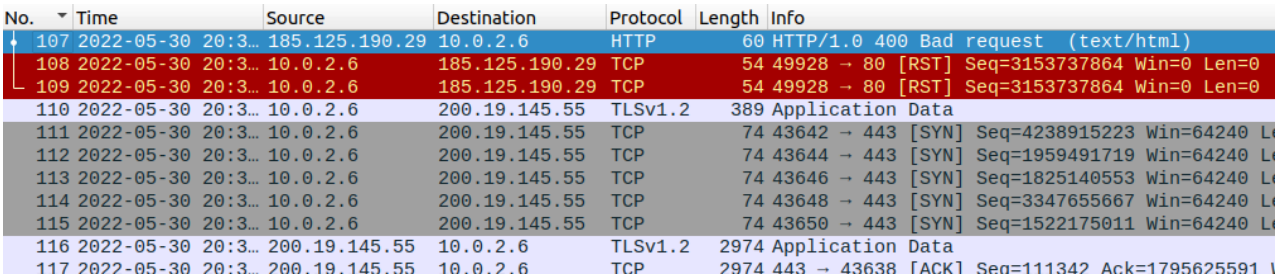
Resolução do item 2)

Wireshark 3.2.3 instalado na máquina virtual.

Resolução do item 3)

A interface gráfica do Wireshark é dividida em três painéis diferentes para inspecionar dados de pacotes.

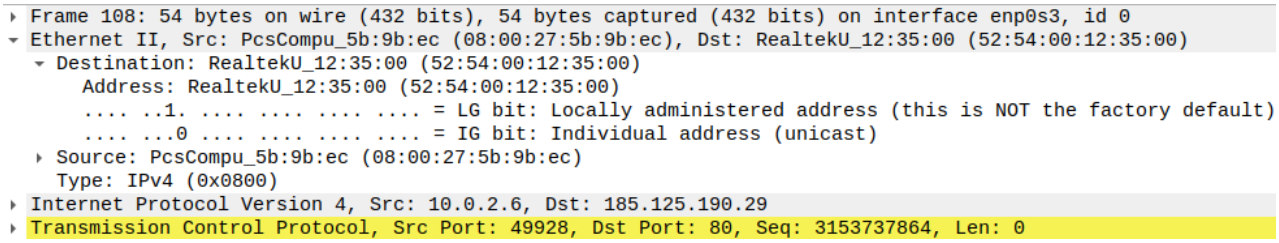
O primeiro painel mostra uma lista com todos os pacotes da captura na rede selecionada. Nessa tela é mostrado a posição numérica do pacote capturado, o tempo que levou do início da captura até a captura do pacote, o endereço IP do remetente e destinatário, o protocolo, o tamanho em bytes e algumas informações extras.



No.	Time	Source	Destination	Protocol	Length	Info
107	2022-05-30 20:3…	185.125.190.29	10.0.2.6	HTTP	60	HTTP/1.0 400 Bad request (text/html)
108	2022-05-30 20:3…	10.0.2.6	185.125.190.29	TCP	54	49928 → 80 [RST] Seq=3153737864 Win=0 Len=0
109	2022-05-30 20:3…	10.0.2.6	185.125.190.29	TCP	54	49928 → 80 [RST] Seq=3153737864 Win=0 Len=0
110	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TLSv1.2	389	Application Data
111	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TCP	74	43642 → 443 [SYN] Seq=4238915223 Win=64240 L
112	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TCP	74	43644 → 443 [SYN] Seq=1959491719 Win=64240 L
113	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TCP	74	43646 → 443 [SYN] Seq=1825140553 Win=64240 L
114	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TCP	74	43648 → 443 [SYN] Seq=3347655667 Win=64240 L
115	2022-05-30 20:3…	10.0.2.6	200.19.145.55	TCP	74	43650 → 443 [SYN] Seq=1522175011 Win=64240 L
116	2022-05-30 20:3…	200.19.145.55	10.0.2.6	TLSv1.2	2974	Application Data
117	2022-05-30 20:3…	200.19.145.55	10.0.2.6	TCP	2974	443 → 43638 [ACK] Seq=111342 Ack=1795625591

Figura 1: Exemplo de Packet List

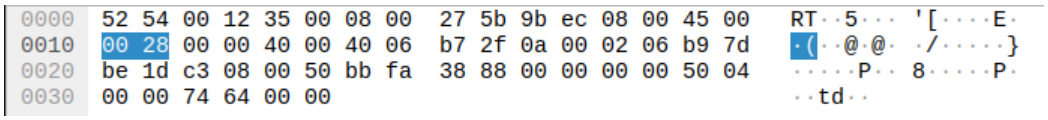
O segundo painel exibe o máximo possível de informações legíveis sobre o pacote selecionado na na primeira tela. Essa informação depende do tipo do pacote selecionado, além de poder expandir a aba de informações, mostrando outras relacionadas.



```
▸ Frame 108: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: PcsCompu_5b:9b:ec (08:00:27:5b:9b:ec), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
  ▾ Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
      Address: RealtekU_12:35:00 (52:54:00:12:35:00)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▸ Source: PcsCompu_5b:9b:ec (08:00:27:5b:9b:ec)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 185.125.190.29
▸ Transmission Control Protocol, Src Port: 49928, Dst Port: 80, Seq: 3153737864, Len: 0
```

Figura 2: Exemplo de Packet Details

O terceiro e último painel exibe o pacote exatamente como ele foi capturado em hexadecimal e em ASCII Dump.



```
0000  52 54 00 12 35 00 08 00  27 5b 9b ec 08 00 45 00   RT··5··· '[····E·
0010  00 28 00 00 40 00 40 06  b7 2f 0a 00 02 06 b9 7d   ·(··@·@· ·/·····}
0020  be 1d c3 08 00 50 bb fa  38 88 00 00 00 00 50 04   ·····P·· 8·····P·
0030  00 00 74 64 00 00                                 ··td··
```

Figura 3: Exemplo de Packet Bytes

Resolução do item 4)

Não consegui utilizar a url www.ufu.br pois estava no https, então utilizei o www.hipertec.com.br.

IP origem: 10.0.2.6
IP destino: 177.12.171.167

Porta origem: 48982
Porta destino: 80
Outras informações estão no repositório.

Resolução do item 5)

Protocolos encontrados:

- TCP: É o principal protocolo de comunicação responsável tanto pelos formatos quanto pelas regras de troca de dados e mensagens entre computadores de uma ou várias redes conectadas à internet.
- HTTP: É um protocolo que especifica como será a comunicação entre um navegador e um servidor web, como o WWW.
- DNS: É um sistema que contém uma lista de nomes de domínio e permite que usuários encontrem uma página por meio desses nomes.
- TLS: É um protocolo de segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores. A diferença entre o 1.2 e o 1.3 é que o último tem velocidades mais rápidas e maior segurança.

Resolução do item 6)

O tempo de demora entre a solicitação feita pelo navegador até a resposta do servidor foi cerca de 0.33387 segundos.

No.	Time	Source	Destination	Protoco	Length	Info
1103	2022/150 22:19:52.224664557	10.0.2.6	177.12.171.167	HTTP	539	GET / HTTP/1.1
1110	2022/150 22:19:52.273573179	177.12.171.167	10.0.2.6	HTTP	288	HTTP/1.1 304 Not Modified
1114	2022/150 22:19:52.426434228	10.0.2.6	177.12.171.167	HTTP	479	GET /css/bootstrap.min.css HTTP/1.1
1119	2022/150 22:19:52.434589568	10.0.2.6	177.12.171.167	HTTP	484	GET /css/bootstrap-theme.min.css HTTP/1.1
1120	2022/150 22:19:52.434753994	10.0.2.6	177.12.171.167	HTTP	481	GET /css/font-awesome.min.css HTTP/1.1
1123	2022/150 22:19:52.461595955	10.0.2.6	177.12.171.167	HTTP	481	GET /css/bootstrap-social.css HTTP/1.1
1124	2022/150 22:19:52.466572505	10.0.2.6	177.12.171.167	HTTP	473	GET /css/mystyles.css HTTP/1.1
1125	2022/150 22:19:52.467326606	177.12.171.167	10.0.2.6	HTTP	318	HTTP/1.1 304 Not Modified
1127	2022/150 22:19:52.469331075	10.0.2.6	177.12.171.167	HTTP	374	GET /js/bootstrap.min.js HTTP/1.1
1131	2022/150 22:19:52.484647078	177.12.171.167	10.0.2.6	HTTP	317	HTTP/1.1 304 Not Modified
1133	2022/150 22:19:52.488597224	177.12.171.167	10.0.2.6	HTTP	317	HTTP/1.1 304 Not Modified
1136	2022/150 22:19:52.504837279	177.12.171.167	10.0.2.6	HTTP	317	HTTP/1.1 304 Not Modified
1147	2022/150 22:19:52.513005553	177.12.171.167	10.0.2.6	HTTP	317	HTTP/1.1 304 Not Modified
1151	2022/150 22:19:52.528533507	10.0.2.6	177.12.171.167	HTTP	387	GET /imagens/Hipertec3.png HTTP/1.1
1167	2022/150 22:19:52.558542909	177.12.171.167	10.0.2.6	HTTP	1136	HTTP/1.1 200 OK (application/javascript)

Figura 4: Tempo entre pacotes

Resolução do item 7)

IP origem: 10.0.2.6
IP destino: 31.13.74.35
Porta origem: 48982
Porta destino: 80
Outras informações estão no repositório.

É possível verificar que existe, comparando com o hipertec e o facebook, semelhanças entre as aplicações, pois ambas se tratam de servidores web. Mas ainda sim é possível observar diferenças entre elas, em que o facebook criptografa alguns dos seus pacotes, melhorando sua segurança.

Parte 2:

IP do coletador: 10.14.94.229
MAC do coletador: 80:56:f2:f4:31:2d

www.msftconnecttest.com
www.msftconnecttest.com/connecttest.txt
v6ncsi.msedge.net

DESKTOP-SPI3STE (Workstation/Redirector)
WORKGROUP
Dropbox Lan

_companion-link._tcp.local
living-room.local
_raop._tcp.local
_airplay._tcp.local
$_{h}ap._tcp.local$
$\_homekit.\_tcp.local$
$F53C6D9F - 38A6 - 5404 - B1C7 - 1CA00D471438.\_homekit.\_tcp.local$
$LivingRoom.\_mediaremotetv.\_tcp.local$
$\_sleep - proxy.\_udp.local$
$pc - mac.\_companion - link.\_tcp.local$

Microsoft-IIS/7.5
Microsoft NCSI

HonHaiPr_f4:31:2d
HewlettP_db:0c:90
Apple_ca:3d:f2
IntelCor_45:37:2e
IPv6mcast_ff:db:0c:90
VMware_9d:67:10
IPv4mcast_7f:ff:fa

Dispositivo: \Device \NPF_ (CCDF7EF5-FB85-4E89-A26A-4D05EA828B60) - Wi-Fi

Protocolos: ARP, DB-LSP-DISC, DHCP, DNS, HTTP, ICMP, MDNS, NBNS, TCP.

Referências

Nakamura E. T. e Geus P. L. de (2007). *Segurança de redes em ambientes cooperativos*. Novatec Editora.