

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

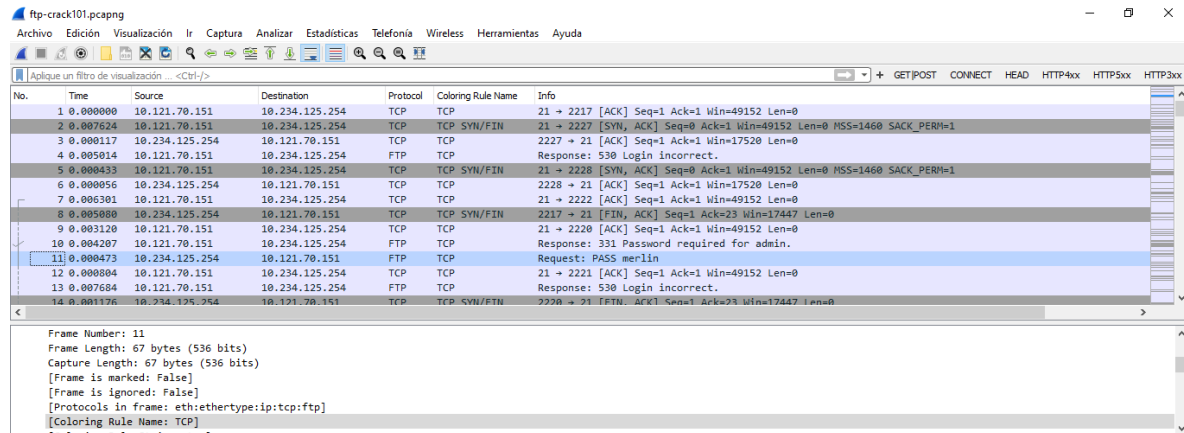
**Lab26 - Build a Coloring Rule to
Highlight FTP User Names, Passwords,
and More**

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab26 - Build a Coloring Rule to Highlight FTP User Names, Passwords, and More

1 Abrimos el archivo ftp-crack101.pcapng. En el paquete 11 podemos observar “Request: PASS merlin”



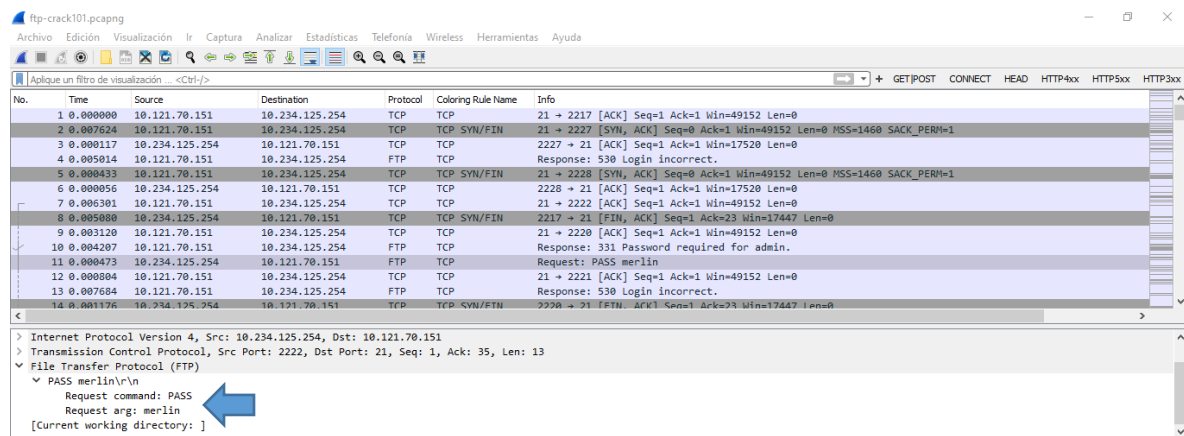
The screenshot shows the Wireshark interface with the file 'ftp-crack101.pcapng' open. The packet list on the left shows packet 11 selected. The packet details pane on the right shows the following information:

- Frame Number: 11
- Frame Length: 67 bytes (536 bits)
- Capture Length: 67 bytes (536 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:ftp]
- [Coloring Rule Name: TCP]

The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Coloring Rule Name	Info
1	0.000000	10.121.70.151	10.234.125.254	TCP	TCP	21 → 2217 [ACK] Seq=1 Ack=1 Win=49152 Len=0
2	0.007624	10.121.70.151	10.234.125.254	TCP	TCP SYN/FIN	21 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
3	0.000117	10.234.125.254	10.121.70.151	TCP	TCP	2227 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.005014	10.121.70.151	10.234.125.254	FTP	TCP	Response: 530 Login incorrect.
5	0.000433	10.121.70.151	10.234.125.254	TCP	TCP SYN/FIN	21 → 2228 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
6	0.000056	10.234.125.254	10.121.70.151	TCP	TCP	2228 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
7	0.006301	10.121.70.151	10.234.125.254	TCP	TCP	21 → 2222 [ACK] Seq=1 Ack=1 Win=49152 Len=0
8	0.005080	10.234.125.254	10.121.70.151	TCP	TCP SYN/FIN	2217 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
9	0.003120	10.121.70.151	10.234.125.254	TCP	TCP	21 → 2220 [ACK] Seq=1 Ack=1 Win=49152 Len=0
10	0.004207	10.121.70.151	10.234.125.254	FTP	TCP	Response: 331 Password required for admin.
11	0.000473	10.234.125.254	10.121.70.151	FTP	TCP	Request: PASS merlin
12	0.000004	10.121.70.151	10.234.125.254	TCP	TCP	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0
13	0.007604	10.121.70.151	10.234.125.254	FTP	TCP	Response: 530 Login incorrect.
14	0.001176	10.234.125.254	10.121.70.151	TCP	TCP SYN/FIN	2220 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0

2 En el paquete 11 nos dirigimos en el panel de detalles y expandimos File Transfer Protocol (FTP). Encontraremos 2 secciones Request Command and Request arg(ument)



The screenshot shows the Wireshark interface with the file 'ftp-crack101.pcapng' open. The packet list on the left shows packet 11 selected. The packet details pane on the right shows the following information:

- Internet Protocol Version 4, Src: 10.234.125.254, Dst: 10.121.70.151
- Transmission Control Protocol, Src Port: 2222, Dst Port: 21, Seq: 1, Ack: 35, Len: 13
- File Transfer Protocol (FTP)
 - PASS merlin\r\n
 - Request command: PASS
 - Request arg: merlin
 - [Current working directory:]

A blue arrow points to the 'Request arg: merlin' field.

ftpr-crack101.pcapng

Archivo Edición Visualización Herramientas Ayuda

Aplicar un filtro de visualización

No. Time Source

1 0.000000 10.1

2 0.007624 10.1

3 0.000117 10.2

4 0.005014 10.1

5 0.000433 10.1

6 0.000056 10.2

7 0.006301 10.1

8 0.005000 10.2

9 0.003120 10.1

10 0.004207 10.1

11 0.000473 10.2

12 0.000004 10.1

13 0.007684 10.1

14 0.001176 10.2

Expand Subtrees
Contraste subárboles
Expandir todo
Contraste todo

Aplicar como columna Control+Mayúsculas+I

Aplicar como filtro

Prepare as Filter

Filtro de conversación

Colorize with Filter

Seguir

Copiar

Mostrar bytes de paquete... Control+Mayúsculas+O

Exportar bytes de paquete... Control+Mayúsculas+X

Wiki Protocol Page

Filter Field Reference

Protocol Preferences

Decodificar como... Control+Mayúsculas+U

Ir a paquete enlazado

Show Linked Packet in New Window

Packet Name Info

21 → 2217 [ACK] Seq=1 Ack=1 Win=49152 Len=0

FIN 21 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1

2227 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0

Response: 530 Login incorrect.

21 → 2227 [ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1

1 Color 1 Ack=1 Win=17520 Len=0

2 Color 2 Ack=1 Win=49152 Len=0

3 Color 3 Seq=1 Ack=23 Win=17447 Len=0

4 Color 4 Ack=1 Win=49152 Len=0

5 Color 5 d required for admin.

6 Color 6 Ack=1 Win=49152 Len=0

7 Color 7 incorrect.

8 Color 8 Seq=1 Ack=23 Win=17447 Len=0

9 Color 9

10 Color 10

Nueva regla de coloreado...

Internet Protocol Version 4
Transmission Control Protocol
File Transfer Protocol
PASS merlin\r\n
Request command
Request arg: me
Current working directory: /

Nombre	Filtro
<input checked="" type="checkbox"/> S-FTP Arguments	ftp.request.arg
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icr
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrpp
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checks
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrpp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

Cambiamos de color el filtro creado a rojo

Wireshark · Reglas de coloreado wireshark101

Nombre	Filtro
<input type="checkbox"/>	
<input checked="" type="checkbox"/> S-FTP Arguments	ftp.request.arg
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icmpv6.type eq 4
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !ip.m ip.m && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !vrrp) (ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !ip.m ip.m && !ospf)
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad"
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

Doble clic para editar. Arrastrar para mover. Las reglas son procesadas en orden hasta que una coincidencia es encontrada.

+ - [Icono] [Icono] Primer plano Fondo Aplicar como filtro

C:\Users\lameri\AppData\Roaming\Wireshark\profiles\wireshark101\colorfilters

Aceptar Copiar desde C Cancelar Import... Export... Ayuda