

questão 1:

Snort: É um IDS de código aberto que pode ser utilizado para a análise de pacotes em tempo real e para a detecção de ataques e sondagens de rede. Ele é amplamente usado devido à sua flexibilidade e eficácia em identificar tráfego de rede suspeito.

Suricata: Outro IDS de código aberto, o Suricata é conhecido por seu desempenho em alta velocidade e suas capacidades avançadas de detecção. Ele pode analisar tráfego de rede, detectar intrusões e até mesmo funcionar como um sistema de prevenção de intrusões (IPS) quando configurado adequadamente.

referências: <https://suricata.io/>, <https://www.snort.org/>

questão 2:

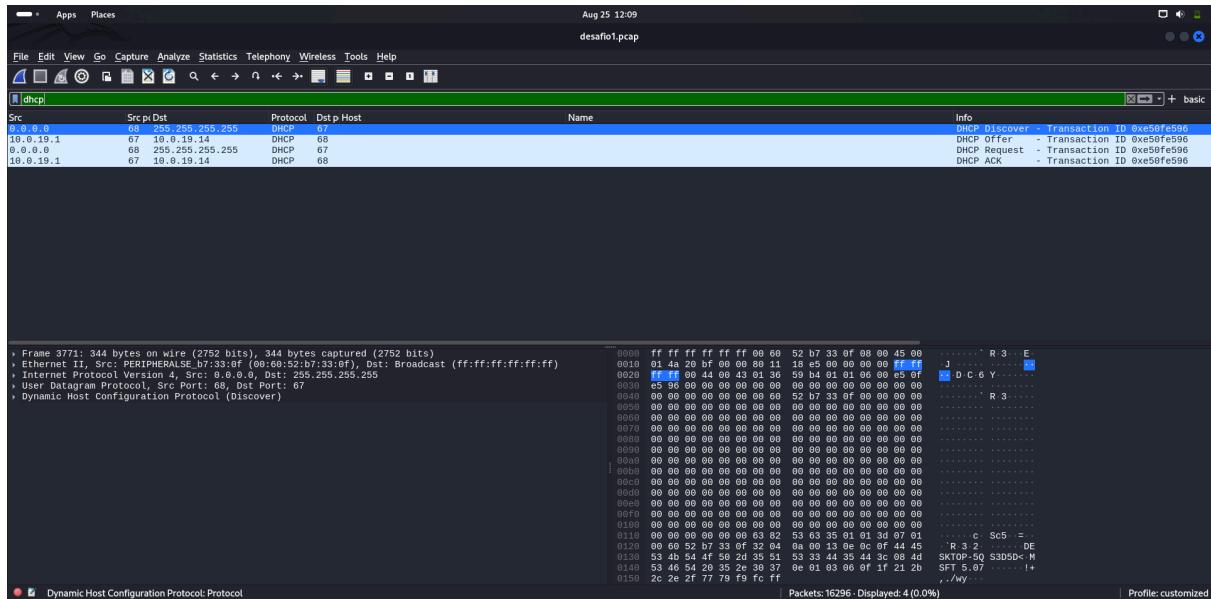
Função Principal:

- **IDS (Sistema de Detecção de Intrusões):** Tem o objetivo de monitorar e identificar atividades suspeitas ou maliciosas na rede ou sistema. Ele gera alertas quando detecta uma possível intrusão, mas não toma ações diretas para bloquear ou prevenir a ameaça.
- **IPS (Sistema de Prevenção de Intrusões):** Além de detectar atividades maliciosas, o IPS pode tomar ações automáticas para prevenir ou bloquear essas ameaças em tempo real. Isso pode incluir o bloqueio de pacotes, o encerramento de sessões ou a reconfiguração de dispositivos de rede.

Ação em Tempo Real:

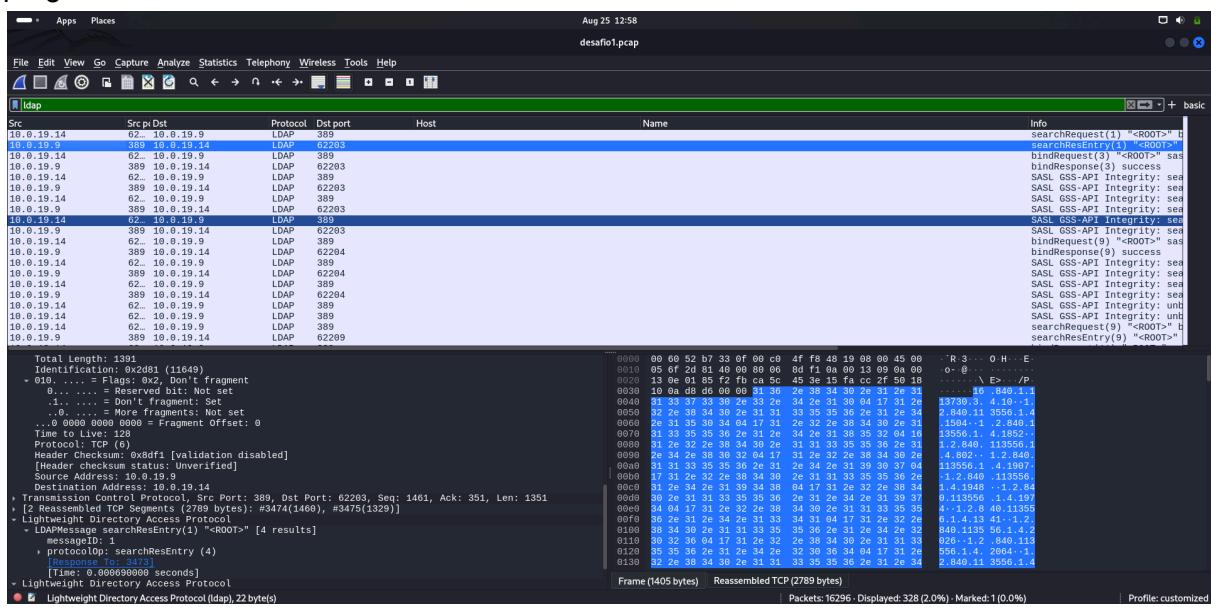
- **IDS:** Opera de forma passiva. Ele monitora e analisa o tráfego, mas não interfere diretamente no tráfego de rede. As ações corretivas devem ser tomadas manualmente por administradores de segurança com base nos alertas gerados.
- **IPS:** Opera de forma ativa. Ele é inserido diretamente no caminho do tráfego de rede e pode interromper, modificar ou redirecionar pacotes suspeitos em tempo real, proporcionando uma defesa mais imediata e automatizada.

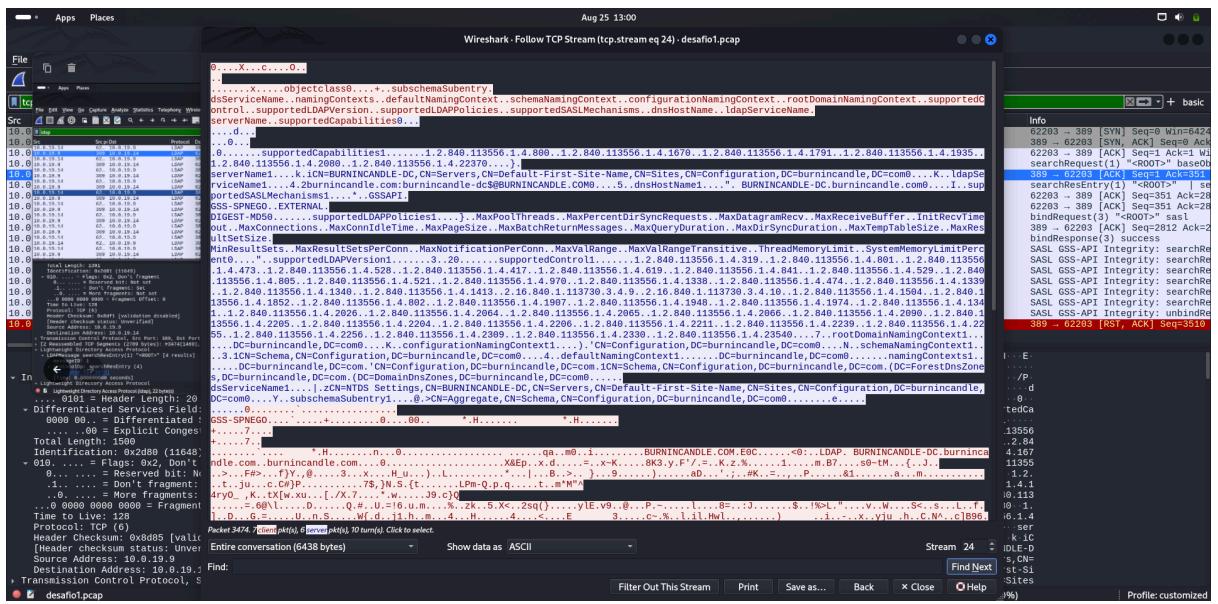
pergunta 3:



IP do servidor DHCP: 10.0.19.1

pergunta 4:





DC = burnincandle-dc

DNS Hostname: O texto menciona "dnsHostName1....". BURNINCANDLE-DC.burnincandle.com, que indica que o nome do host do servidor é "BURNINCANDLE-DC" e pertence ao domínio "burnincandle.com".

LDAP Service Name: A linha

"ldapServiceName1....4.2burnincandle.com:burnincandle-dc\$@BURNINCANDLE.COM" mostra que o serviço LDAP está associado ao domínio "burnincandle.com", reforçando que este domínio é gerido pelo servidor "burnincandle-dc".

Server Name:

"serverName1....k.iCN=BURNINCANDLE-DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration,DC=burnincandle,DC=com". Isso mostra que o servidor controlador é identificado como "BURNINCANDLE-DC" dentro do contexto de configuração do domínio "burnincandle.com".

Pergunta 5:

Screenshot of Wireshark showing network traffic analysis. The packet list shows various connections to bing.com, checkapex.microsoft.com, www.bing.com, antnosience.com, filebin.net, and situla.bitbin.net. The details and bytes panes show the structure of the captured packets.

```

Aug 25 13:09
desafio1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[http://tts.handshake.type.eq1
Src Src & Dst Protocol Dst port Host Name Info
10.0.19.14 62...294.79.197.200 TLSv1.2 443 www.bing.com Client Hello (SNI=www.bing...
10.0.19.14 62...13.107.136.254 TLSv1.2 443 spo-riing.msedge.net Client Hello (SNI=spo-ri...
10.0.19.14 62...294.79.197.200 TLSv1.2 443 www.bing.com Client Hello (SNI=www.bing...
10.0.19.14 62...29.81.51.95 TLSv1.2 443 checkapex.microsoft.com Client Hello (SNI=checkap...
10.0.19.14 62...294.79.197.200 TLSv1.2 443 www.bing.com Client Hello (SNI=www.bing...
10.0.19.14 62...157.245.142.66 TLSv1.2 443 antnosience.com Client Hello (SNI=antnosie...
10.0.19.14 62...157.245.142.66 TLSv1.2 443 antnosience.com Client Hello (SNI=antnosie...
10.0.19.14 62...185.47.40.36 TLSv1.2 443 filebin.net Client Hello (SNI=filebin...
10.0.19.14 62...87.238.33.8 TLSv1.2 443 situla.bitbin.net Client Hello (SNI=situla.bi...
10.0.19.14 62...184.80.96.219 HTTP 80 r3.i-lener.org Client Hello (SNI=r3.i-lener...
10.0.19.14 62...19.8.14 HTTP 62259 budupdate.com GET / HTTP/1.1
10.0.19.14 62...23.227.198.203 TLSv1.2 757 budupdate.com HTTP/1.1 200 OK (application/x-...
10.0.19.14 62...23.227.198.203 TLSv1.2 757 budupdate.com Client Hello (SNI=budupdate...
10.0.19.14 62...23.227.198.203 TLSv1.2 757 budupdate.com Client Hello (SNI=budupdate...
10.0.19.14 62...13.69.116.104 TLSv1.2 443 v10.events.data.microsoft.com Client Hello (SNI=v10.event...
10.0.19.14 62...52.183.220.149 TLSv1.2 443 settings-win.data.microsoft.com Client Hello (SNI=settings-wi...

```

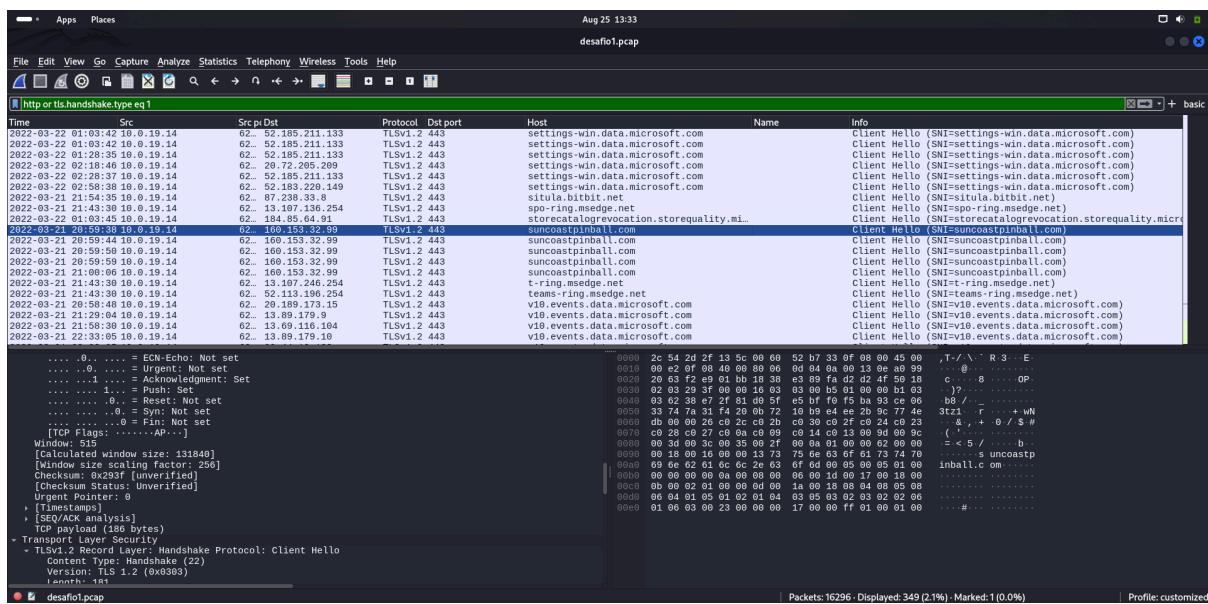
Frame 4: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) Encapsulation type: Ethernet (1) Arrival Time: Mar 23 2024 17:18:08.049000 -03 Arriving Interface: Intel PRO/100 MT Desktop 20:58:11.303499000 UTC Epoch Arrival Time: 1647996291.303499000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000000000 seconds] [Time since reference or first frame: 0.160751000 seconds] [Time since previous frame: 0.000000000 seconds] Frame Number: 4 Frame Length: 365 bytes (2920 bits) Encapsulation Bits: 0x0000 (Ethernet II) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ether:ip:tcp:http] [Decoding Rule String: http [tcp port == 80 || http2]] [Coloring Rule String: PERIPHERAL_b7:33:0f (08:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)] -> Destination: Cisco_2f:13:5c (2c:54:2d:2f:13:5c) Address: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)0 = 0 bit: Globally unique address (factory default)0 = 0 bit: Individual address (unicast)

A conexão pra bupdater.com é suspeita, olhando a porta vemos que é 757 e não 80 ou 443 e filtrei por http ou https. Olhando na internet, no site virustotal.com analisei o domínio:

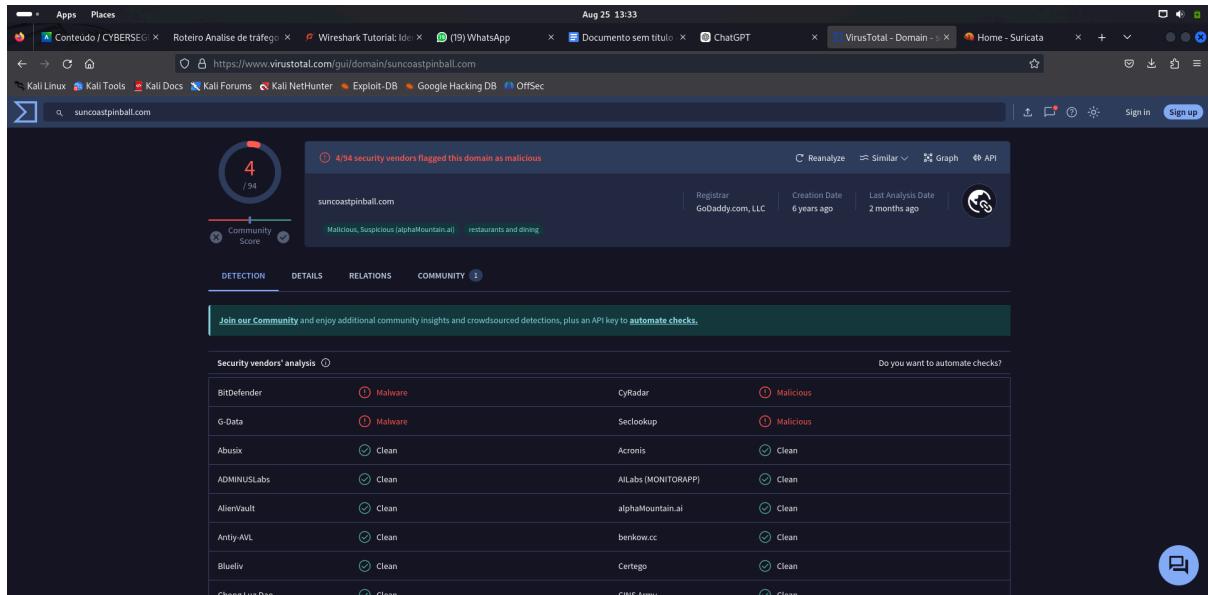
Screenshot of VirusTotal analysis for <http://bupdater.com>. The analysis shows a score of 6/96 security vendors flagged this URL as malicious. The detection section lists various security vendors and their findings. The community section encourages joining the community and automating checks.

Security vendor	Result
Anti-AVL	Malicious
CyRadar	Malicious
Sectlookup	Malicious
Abusix	Clean
ADMINUSlabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BlockList	Clean
BitDefender	Malware
G-Data	Malware
Sophos	Malware
Acronis	Clean
AI Labs (MONITORAPP)	Clean
alphaMountain.ai	Clean
benkow.cc	Clean
Blueliv	Clean

Outra conexão suspeita foi a de baixo:



verificando no virustotal.com:



pergunta 6: 90:b1:1c:96:d2:c8

Aug 25 13:39
desafio2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Info
2018-11-13 01:59:39	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP Inform
2018-11-13 02:02:19	192.168.2.147	68	192.168.2.147	DHCP	67			DHCP ACK
2018-11-13 02:02:19	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP Inform
2018-11-13 02:02:19	192.168.2.4	67	192.168.2.147	DHCP	68			DHCP ACK

```

Frame 386: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Dell_9e:02:c8 (90:b1:1c:96:d2:c8), Dst: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
  Destination: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
  Source: Dell_9e:02:c8 (90:b1:1c:96:d2:c8)
    Address: Dell_9e:02:c8 (90:b1:1c:96:d2:c8)
      ... .0 .. . = L6 bit: Globally unique address (factory default)
      ... .0 .. . = Ig bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.2.4, Dst: 192.168.2.147
  User Datagram Protocol, Src Port: 67, Dst Port: 68
    Destination Port: 68
    Length: 368
    Checksum: 0xc8ef [unverified]
      [Checksum Status: Unverified]
      [Timestamp Index: 17]
    > [Timestamps]
    UDP payload (368 bytes)
> Dynamic Host Configuration Protocol (ACK)
  Source or Destination Hardware Address (eth.addr), 6 byte(s)

```

Packets: 1541 - Displayed: 4 (0.3%) | Profile: customized

pergunta 7: bc:5f:f4:a6:d1:29

Aug 25 13:40
desafio2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Info
2018-11-13 01:59:39	192.168.2.4	68	255.255.255.255	DHCP	67			DHCP Inform
2018-11-13 02:02:13	192.168.2.147	68	255.255.255.255	DHCP	67			DHCP ACK
2018-11-13 02:02:13	192.168.2.4	67	192.168.2.147	DHCP	68			DHCP Inform

```

Frame 385: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Address: Broadcast (ff:ff:ff:ff:ff:ff)
    ... .A .. . = L6 bit: Locally administered address (this is NOT the factory default)
    ... .1 .. . = Ig bit: Group address (multicast/broadcast)
  Source: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
    Address: ASRockIncorp_a6:d1:29 (bc:5f:f4:a6:d1:29)
      ... .0 .. . = L6 bit: Globally unique address (factory default)
      ... .0 .. . = Ig bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.2.147, Dst: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
    Destination Port: 67
    Length: 368
    Checksum: 0x88c8 [unverified]
      [Checksum Status: Unverified]
      [Timestamp Index: 16]
    > [Timestamps]
    UDP payload (368 bytes)
> Dynamic Host Configuration Protocol (Inform)
  Source or Destination Hardware Address (eth.addr), 6 byte(s)

```

Packets: 1541 - Displayed: 4 (0.3%) | Profile: customized

pergunta 8:Host=LYAKH-WIN7-PC

Aug 25 14:00
desafio2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

cldap

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Text item	Info
2018-11-13 01:59:36	192.168.2.147	57	192.168.2.4	CLDAP	389			/	se
2018-11-13 01:59:36	192.168.2.4	389	192.168.2.147	CLDAP	57576			/	se
2018-11-13 01:59:36	192.168.2.147	57	192.168.2.4	CLDAP	389			/	se
2018-11-13 01:59:37	192.168.2.147	389	192.168.2.147	CLDAP	57571			/	se
2018-11-13 01:59:37	192.168.2.147	57	192.168.2.4	CLDAP	389			/	se
2018-11-13 01:59:37	192.168.2.147	389	192.168.2.147	CLDAP	56110			/	se
2018-11-13 01:59:37	192.168.2.147	53	192.168.2.4	CLDAP	389			/	se
2018-11-13 01:59:37	192.168.2.147	389	192.168.2.147	CLDAP	53443			/	se
2018-11-13 01:59:37	192.168.2.147	55	192.168.2.4	CLDAP	389			/	se
2018-11-13 01:59:37	192.168.2.147	389	192.168.2.147	CLDAP	59850			/	se

[Stream index: 5]
[Timestamps]
+ UDP payload (172 bytes)
+ Connectionless Lightweight Directory Access Protocol
+ LDAPmessage searchRequest(1) <R00T> baseObject
+ messageID: 1
+ protocolSearchRequest ()
+ searchRequest:
+ baseObject:
+ scope: baseObject ()
+ derefAliases: neverDerefAliases ()
+ sizeLimit: 0
+ timeLimit: 0
+ typesOnly: False
+ Filter: (&&(&(dnsDomain=dniproductors.com.)(Host=LYAKH-WIN7-PC))(DomainGuid=006b589e-dfe7-46...
+ and: (&(&(dnsDomain=dniproductors.com.)(Host=LYAKH-WIN7-PC))(DomainGuid=006b589e-dfe7-46...
+ and: 4 items
+ and: (dnsDomain=dniproductors.com.)
+ and: itemMatchFilterMatch (3)
+ equalityMatch
+ attributeDesc: DnsDomain

Packets: 1541 - Displayed: 10 (0.6%) | Profile: customized

Pergunta 9: jermija.lyakh

Aug 25 14:23
desafio2.pcap

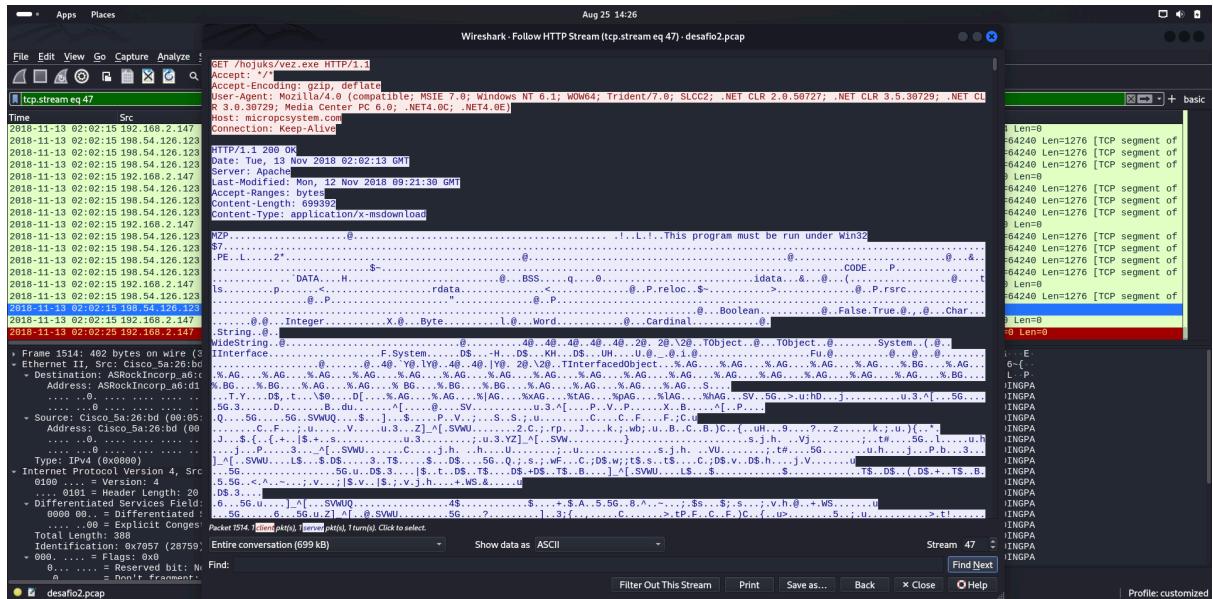
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos

Time	Src	Src port	Dst	Protocol	Dst port	Host	NaiText item	CNameString	Info
2018-11-13 01:59:47	192.168.2.4	389	192.168.2.147	KRB5	49186		/	LYAKH-WIN7-PCS	bindResponse(10) success
2018-11-13 01:59:47	192.168.2.147	49	192.168.2.4	KRB5	88		/	LYAKH-WIN7-PCS	AS-REQ
2018-11-13 01:59:47	192.168.2.147	88	192.168.2.4	KRB5	49187		/	LYAKH-WIN7-PCS	KRB_Error: KRB5KDC_ERR_PREAMTH_REQUIRED
2018-11-13 01:59:47	192.168.2.147	49	192.168.2.4	KRB5	88		/	LYAKH-WIN7-PCS	AS-REQ
2018-11-13 01:59:47	192.168.2.147	88	192.168.2.4	KRB5	49188		/	LYAKH-WIN7-PCS	AS-REP
2018-11-13 01:59:47	192.168.2.147	49	192.168.2.4	KRB5	88		/	LYAKH-WIN7-PCS	TGS-REQ
2018-11-13 01:59:47	192.168.2.147	88	192.168.2.4	KRB5	49189		/	LYAKH-WIN7-PCS	TGS-REP
2018-11-13 02:01:45	192.168.2.147	49	192.168.2.4	KRB5	88		/	jermija.lyakh	AS-REQ
2018-11-13 02:01:45	192.168.2.147	89	192.168.2.147	KRB5	49192		/	jermija.lyakh	KRB_Error: KRB5KDC_ERR_PREAMTH_REQUIRED
2018-11-13 02:01:45	192.168.2.147	49	192.168.2.4	KRB5	88		/	jermija.lyakh	AS-REQ
2018-11-13 02:01:45	192.168.2.147	89	192.168.2.147	KRB5	49193		/	jermija.lyakh	AS-REP
2018-11-13 02:01:45	192.168.2.147	49	192.168.2.4	KRB5	88		/	jermija.lyakh	TGS-REQ
2018-11-13 02:01:45	192.168.2.147	88	192.168.2.147	KRB5	49194		/	jermija.lyakh	TGS-REP
2018-11-13 02:01:46	192.168.2.147	49	192.168.2.4	KRB5	88		/	jermija.lyakh	TGS-REQ
2018-11-13 02:01:46	192.168.2.147	88	192.168.2.147	KRB5	49197		/	jermija.lyakh	TGS-REP
2018-11-13 02:01:46	192.168.2.147	49	192.168.2.4	DCERPC	49155		/		Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI_V4_0 (32011 NDR Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5640 max_recv: 5640, 3 res Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI_V4_0 (
2018-11-13 02:01:46	192.168.2.147	49	192.168.2.4	DCERPC	49196		/		
2018-11-13 02:01:46	192.168.2.147	49	192.168.2.4	DCERPC	49155		/		
as-rep									
pwno: 5									
realm: krb-as-rep (11)									
adata: 1 item									
crealm: DNIPROMOTORS.COM									
+ cname									
+ name-type: kRB5_NT_PRINCIPAL (1)									
+ cname-string: 1 item									
+ CNameString: jermija.lyakh									
+ ticket									
+ auth-type: 5									
+ realm: DNIPROMOTORS.COM									
+ sname									
+ name-type: KRB5_NT_SRV_INST (2)									
+ SNameString: krbtgt									
+ SNameString: DNIPROMOTORS.COM									
+ enc-part									
+ type: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)									
+ keysize: 2									
+ cipher: [truncated]: fce2448be13983d737ce2f24ed49386876a13fd8fa1ff52b0c58d6dcba4339ff4eb3c5a73c5									
+ enc-part									
Frame (224 bytes) Reassembled TCP (1630 bytes)									

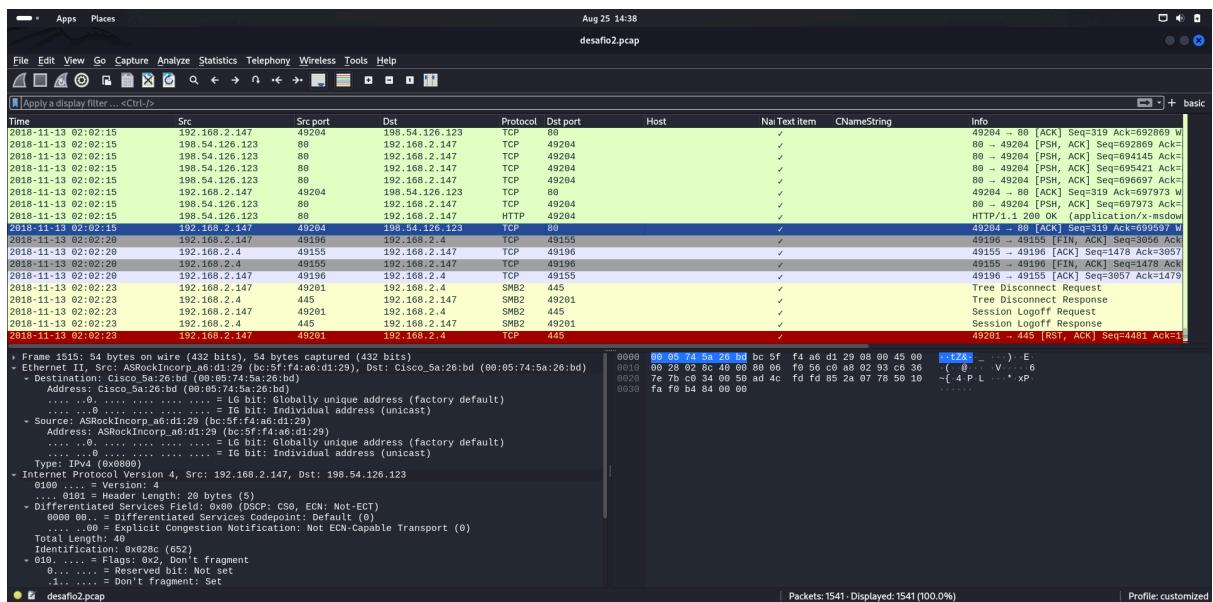
Packets: 1541 - Displayed: 76 (4.9%) | Profile: customized

Resposta 10: micropcsystem.com/hojuks/vez.exe o nome do arquivo é vez.exe



Resposta 11: 2018-11-13 02:02:13

Resposta 12: 198.54.126.123



Resposta 13: 00:1e:67:4a:d7:5c

Aug 25 14:43
desafio3.pcap

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[ ip.addr == 172.17.1.129 ] basic
Time Src Src/Dst Protocol Dstport Host NaiText Item CNameString Info
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB NALYVAIKO-PC<0>
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB KYIVARTWORKS<0>
2018-11-12 21:01:15 172.17.1.129 60.. 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 66888 -- Standard query response 0x109 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 59478 -- Standard query response 0x109 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 DNS 53 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.129 DNS 53548 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53556 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53552 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49156 .. 49156 [SYN] Seq=0 Win=0 MSS=1468
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 TCP 49155 -- 49155 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49155 .. 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.129 DCERPC 135 Bind: call_id: 2, Fragment: Single, 3 context it
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 DCERPC 49155 Bind: ack: call_id: 2, Fragment: Single, max_xmit
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 EPM 135 Map request, RPC_NETLOGON, 32bit NDR

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Intel 4a:d7:5c (00:1e:67:4a:d7:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
Address: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
..... . . . . . = L6 bit: Globally unique address (factory default)
..... . . . . . = I6 bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.1.129, Dst: 172.17.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Flags: 0x0000, 0x0000
Flags: 0x0000, 0x0000
Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  - NALYVAIKO-PC<0>: type NB, class IN
    Name: NALYVAIKO-PC<0> (Workstation/Redirector)
    Type: NB (32)
    Class: IN (1)
Source Hardware Address (eth.src), 6 byte(s)

```

Packets: 19928 - Displayed: 19928 (100.0%) | Profile: customized

Resposta 14: NALYVAIKO-PC

Aug 25 14:43
desafio3.pcap

```

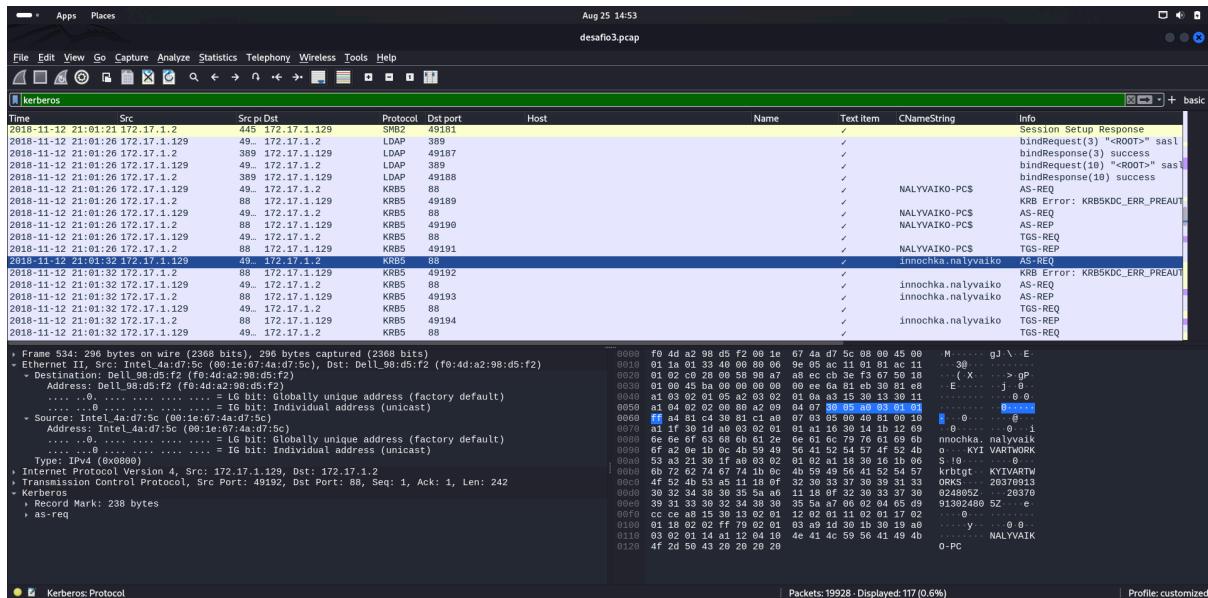
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[ ip.addr == 172.17.1.129 ] basic
Time Src Src/Dst Protocol Dstport Host NaiText Item CNameString Info
2018-11-12 21:01:15 172.17.1.129 137 172.17.1.255 NBNS 137 ✓ Registration NB NALYVAIKO-PC<0>
2018-11-12 21:01:15 172.17.1.129 60.. 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 66888 -- Standard query response 0x109 SRV _ldap._tcp.dc._msdcs.KYIVARTWORKS
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.2 DNS 53 -- Standard query 0x108 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53 172.17.1.129 DNS 59478 -- Standard query response 0x109 SRV _ldap._tcp.Default-Fqdn
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 DNS 53 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.129 DNS 53548 k_.. Standard query response 0x1ab4 A kyivartworks-dc.kyivartworks
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53556 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 53.. 172.17.1.2 CLDAP 389 ✓ searchRequest(1) "<ROOT>" baseObject
2018-11-12 21:01:15 172.17.1.129 389 172.17.1.129 CLDAP 53552 ✓ searchResEntry(1) "<ROOT>" searchResDone(1) success
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49156 .. 49156 [SYN] Seq=0 Win=0 MSS=1468
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 TCP 49155 -- 49155 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 TCP 135 ✓ 49155 .. 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.129 DCERPC 135 Bind: call_id: 2, Fragment: Single, 3 context it
2018-11-12 21:01:15 172.17.1.129 135 172.17.1.129 DCERPC 49155 Bind: ack: call_id: 2, Fragment: Single, max_xmit
2018-11-12 21:01:15 172.17.1.129 49.. 172.17.1.2 EPM 135 Map request, RPC_NETLOGON, 32bit NDR

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Intel 4a:d7:5c (00:1e:67:4a:d7:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
Address: Intel 4a:d7:5c (00:1e:67:4a:d7:5c)
..... . . . . . = L6 bit: Globally unique address (factory default)
..... . . . . . = I6 bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.1.129, Dst: 172.17.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Flags: 0x0000, 0x0000
Flags: 0x0000, 0x0000
Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  - NALYVAIKO-PC<0>: type NB, class IN
    Name: NALYVAIKO-PC<0> (Workstation/Redirector)
    Type: NB (32)
    Class: IN (1)
Source Hardware Address (eth.src), 6 byte(s)

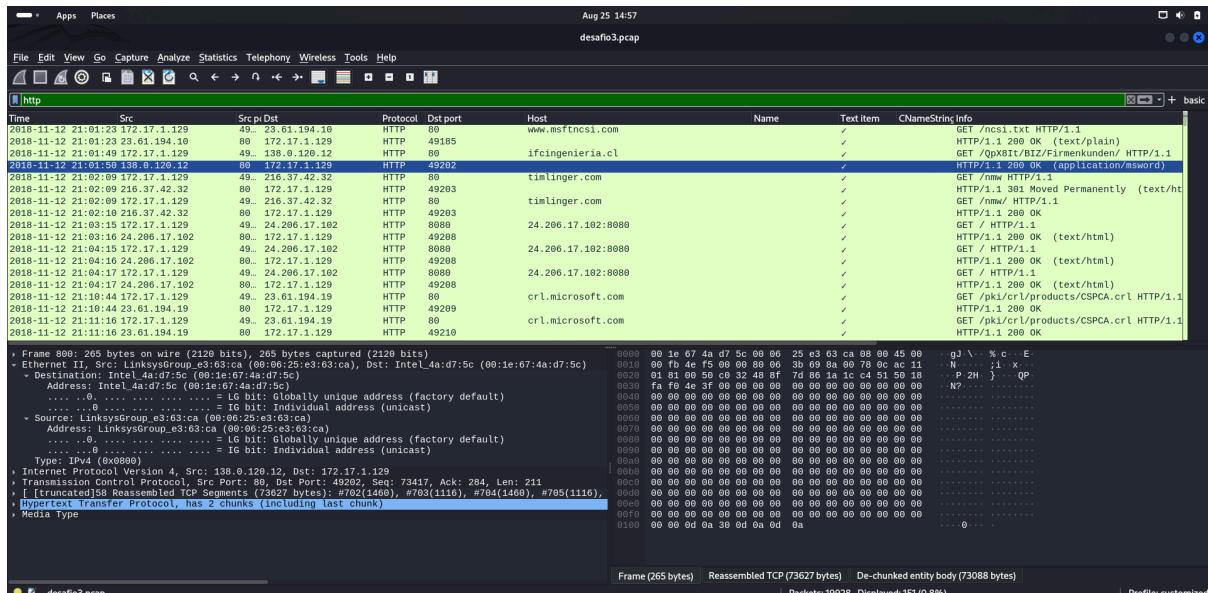
```

Packets: 19928 - Displayed: 19928 (100.0%) | Profile: customized

Resposta 15: innochka.nalyvaiko



Resposta 16:<http://ifcingenieria.cl/QpX8lt/BIZ/Firmenkunden>



Pergunta 17:

data de acesso:2018-11-12 21:01:49

Pergunta 18:timlinger.com/nmw/ retornou o eecutável 6169583.exe

Resposta 19: 192.168.1.2

Resposta 20:steve.smith

The screenshot displays a network capture in Wireshark. The timeline pane shows a sequence of four Kerberos messages exchanged between a client and a server. The packet details pane provides a detailed view of each message's structure, including fields like Src, Dst, Protocol, and Data. The bytes pane shows the raw binary data for each message. A specific packet, the AS-REP message containing the user name 'steve.smith', is highlighted in blue. The status bar at the bottom indicates the total number of packets (5880) and the display filter (9.1% of the total).

Pergunta 21:desktop-gxmyno2

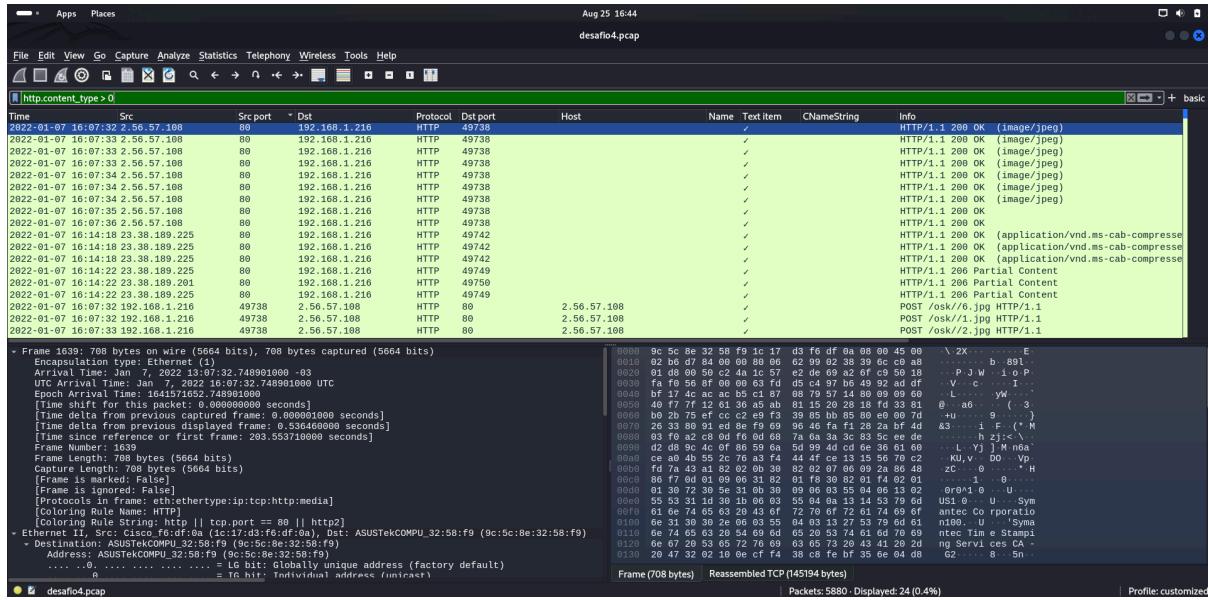
The screenshot shows a network capture in Wireshark. The timeline pane at the top indicates the capture was taken on Aug 25 15:47 from file desfa04.pcap. The packet list pane shows 5880 total packets, with 97 displayed. The selected packet is a Kerberos ticket grant request (TGS-REQ) from the client to the server. The packet details pane shows the structure of the Kerberos message, including fields like 'Protocol' (KRB5), 'Dst Port' (46457), 'Host' (krbtgt/krbtgt), and 'Text Item' (Ticket Granting Service). The bytes pane shows the raw binary data of the message. The bottom status bar indicates the profile is 'basic'.

Pergunta 22:

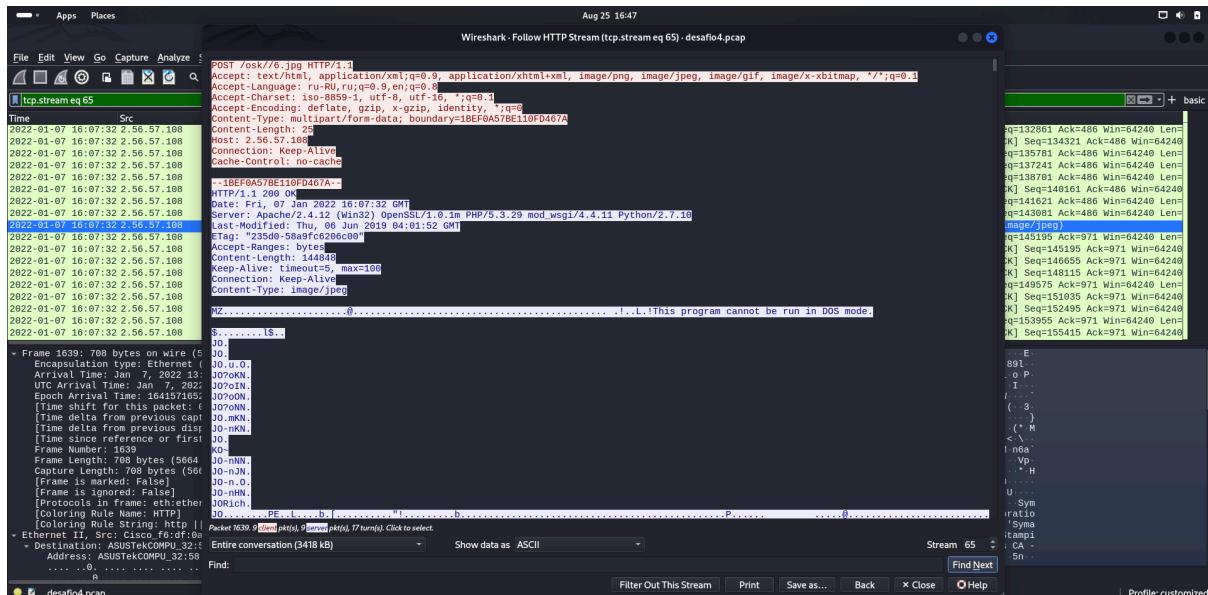
Primeiro podemos ver que o ip 192.168.1.216 fez vários posts suspeitos pro ip 2.56.57.108, são suspeitos porque podemos ver que o content type é image/jpeg mas como vemos abaixo ele está enviando um arquivo que começa com MZ, que é provavelmente um arquivo executável windows.

POST /osk/.6.jpg HTTP/1.1
Content-Type: multipart/form-data; boundary=BEF0A57BE10F4D67A
Accept: */*
Accept-Language: en-US;q=0.9, application/xhtml+xml;q=0.8, image/png;q=0.7, image/jpeg;q=0.6, image/gif;q=0.5, image/x-bitmap;q=0.4, */*;q=0.1
Accept-Charset: iso-8859-1;q=0.9, utf-8;q=0.8, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=BEF0A57BE10F4D67A
Time: 2022-01-07 16:07:32.565718000
Host: 2.56.57.108
Connection: Keep-Alive
Cache-Control: no-cache
Content-Type: multipart/form-data; boundary=BEF0A57BE10F4D67A--
HTTP/1.1 299 OK
Date: Fri, 07 Jan 2022 16:07:32 GMT
Server: Apache/2.4.41 (Ubuntu) OpenSSL/1.1.1 PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.16
Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT
Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT
Accept: "235d0:c6206c80"
Accept-Ranges: bytes
Content-Length: 708
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpg0
M2.....@.....!..L.!This program cannot be run in DOS mode.
Frame 1639: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) on interface Ethernet 0
Encapsulation type: Ethernet (Arrival Time: Jan 7, 2022, 13:00:40.000000000 +0000)
Source: Cisco f6/df:8e (00:0c:29:f6:df:8e)
Epoch Arrival Time: 1641571653.000000000 [Time shift for this packet: 0]
[Time delta from previous capture: 0.000000000]
[Time delta from previous display: 0.000000000]
[Time since reference or first frame: 1639]
Frame Number: 1639
Frame Length: 708 bytes (5664 bits)
Capture Length: 708 bytes (5664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethernet (ethernet II) / ip / tcp / http]
[Coloring Rule String: http://]
Ethernet II, Src: Cisco f6/df:8e (00:0c:29:f6:df:8e), Dst: ASUSTek COMPUTER_32:5B (00:0c:29:32:5b:00)
Destination: ASUSTek COMPUTER_32:5B (00:0c:29:32:5b:00)
Find: Stream 65 Find Next

Logo depois vemos a máquina de destino retornar pra máquina de ip 192.168.1.216 arquivos suspeitos também:



Podemos ver que o content type é image/jpeg mas se olharmos no conteúdo, vamos ver que começa com MZ indicando ser um arquivo executável de windows ou um dll:



podemos salvar o conteúdo e ver com o comando file o tipo de arquivo, se é uma jpeg ou um executável ou dll:

Aug 25 18:01
fernando@fernando: ~/Downloads

```
[fernando@fernando:~/Downloads]
└─$ file 6.jpg
6.jpg: PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections
[fernando@fernando:~/Downloads]
```

Arquivo Editar Ver inserir Formatar Ferramentas Extensões Ajuda

Podemos ver que o content type é image/jpeg mas se olharmos no conteúdo, vamos ver que começa com MZ, indicando ser um arquivo executável de windows ou um dll.

podemos salvar o conteúdo e ver com o comando file o tipo de arquivo, se é um jpg ou um executável ou dll.

Pergunta 23:
Como podemos ver na imagem abaixo, o ip que retorna arquivos suspeitos é o 2.56.57.108 como mostrado abaixo:

vemos que é um dll e não um jpg, portanto é uma conexão suspeita.

Pergunta 23:

Como podemos ver na imagem abaixo, o ip que retorna arquivos suspeitos é o 2.56.57.108 como mostrado abaixo:

Aug 25 16:50
desafio4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.content_type > 0

Time	Src	Src port	Dst	Protocol	Dst port	Host	Name	Text item	CNameString	Info
2022-01-07 16:07:34 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK (image/jpeg)
2022-01-07 16:07:35 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK
2022-01-07 16:07:36 2.56.57.108	80	192.168.1.216		HTTP	49738					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:18 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:19 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2022-01-07 16:14:20 23.38.189.225	80	192.168.1.216		HTTP	49742					HTTP/1.1 200 Partial Content
2022-01-07 16:14:22 23.38.189.225	80	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:14:23 23.38.189.225	80	192.168.1.216		HTTP	49750					HTTP/1.1 206 Partial Content
2022-01-07 16:14:22 23.38.189.225	80	192.168.1.216		HTTP	49749					HTTP/1.1 206 Partial Content
2022-01-07 16:07:32 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/6.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/2/3.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/3.jpg HTTP/1.1
2022-01-07 16:07:33 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/4.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/5.jpg HTTP/1.1
2022-01-07 16:07:34 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/7.jpg HTTP/1.1
2022-01-07 16:07:35 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/main.php HTTP/1.1
2022-01-07 16:07:36 192.168.1.216	49738	2.56.57.108		HTTP	80	2.56.57.108				POST /osk/HTTP/1.1 (zip)

- Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jan 7, 2022 13:07:32.212441000 -03
Epoch Arrival Time: 1641571652.212441000 UTC
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000431000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 263.017250000 seconds]
Frame Number: 1501
Frame Length: 539 bytes (4312 bits)
Encapsulation type: Ethernet (4312 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ether:type:ip:tcp:http:mime multipart]
[Containing Rule String: http || tcp port == 80 || http2]
[Containing Rule String: http || tcp port == 80 || http2]
- Ethernet II, Src: ASUSTekCOMPU_32:58:f9 (0c:5c:8e:32:58:f9), Dst: Cisco_f0:df:0a (1c:17:d3:f6:df:0a)
- Destination: Cisco_f0:df:0a (1c:17:d3:f6:df:0a)
Address: Cisco_f0:df:0a (1c:17:d3:f6:df:0a)
.....0.....16 bits probably unique address (factory default)
.....0.....a = Tc hit: Individual address (unicast)

0000 1c 17 d3 f6 df 0a 9c 5c 8e 32 58 f9 08 00 45 96 \ 2X .. E
0010 02 0d cd 68 48 08 80 28 50 c0 a8 01 d8 02 38 h... .A... 8
0020 39 6c 24 a0 08 59 62 6d e4 1c 55 ae 42 50 18 91 J R m A B
0030 2f 30 2e 6a 70 57 49 48 54 54 50 2f 31 2e 31 0d /6.jpg H TIP/1.1
0040 0f 6d 2c 29 51 78 78 8c 69 63 61 74 69 67 6e 5e , m_appli_cation/
0050 0a 41 63 65 70 74 3a 20 74 65 78 74 2f 67 74 Accept: text/ht
0060 06 6c 2c 29 51 78 78 8c 69 63 61 74 69 67 6e 5e , m_appli_cation/
0070 03 61 74 69 67 6e 2f 78 68 74 6d 6c 28 78 6d 6c , m_appli_cation/x_html+xml
0080 2c 20 69 6d 61 67 65 2f 70 66 67 2c 28 69 6d 61 , image/png, ima
0090 67 65 2f 6a 68 67 62 29 69 6d 61 67 65 2f 67 ge/jpeg, image/g
0100 6d 61 70 2c 28 24 2f 38 71 3d 30 2e 31 0d 0a , image/x_gif
0000 6d 61 70 2c 28 24 2f 38 71 3d 30 2e 31 0d 0a map/1/1-q0=1
0010 41 63 63 65 70 74 2d 4c 61 6b 67 75 61 67 63 3a Accept-L anguage:
0020 2d 72 75 2d 52 55 2c 72 75 3d 71 3d 30 2e 39 2c ru-Ru, r_uq=0.9,
0030 05 6c 30 2e 31 0d 0a 08 03 05 6c 30 2e 39 2c opengraph: Acepted
0040 03 61 6b 67 75 3d 71 73 74 3d 60 63 67 6f 59 38 , Chars : 10888
0050 35 39 2d 31 2c 28 75 74 66 2d 38 2c 26 75 74 66 59-1, ut f-8, utf
0120 2d 31 36 2c 28 2a 30 71 3d 30 2e 31 0d 0a 41 63 , ' ; q=1. Ac
0130 63 65 2c 28 2a 30 71 3d 30 2e 31 0d 0a 41 63 , opengraph: d
0140 6d 61 6b 67 75 3d 71 73 74 3d 60 63 67 6f 59 38 , opengraph: oodmg: d
0150 67 79 69 78 2c 29 69 64 65 66 74 69 74 79 2c 28 gzip, id entity,

Packets: 5880 - Displayed: 24 (0.4%)

Profile: customized

Vemos que a porta de conexão foi feita na porta 80.