Appunti ed esercizi esame svolti - Wireshark con correzioni

Sicurezza dei sistemi e delle reti (Università degli Studi di Milano)

24/01/2017

Esaminando il traffico reso disponibile alla pagina:

rispondere alle domande nello spazio predisposto.

1. Quali nodi IP sono sorgente o destinazione di traffico? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

2. Quali sono le richieste scambiate con browser e quali sono i numeri dei pacchetti coinvolti. Quali sono gli URI degli oggetti scambiati?
    a. In risposta il server, restituisce un file: in che linguaggio è scritto il file?

    b. Nel file viene costruito un Array, quanto è lungo e che etichetta ha?

    c. Che valore hanno i suoi elementi?

3. Nel pacchetto n. 17, si sa che il server restituisce al client un malware: sai dire quando inizia la conversazione client-server e che tipo di programma viene inviato?

1. Quali nodi IP sono sorgente o destinazione di fraffico? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

Risposta

ho trovato due nodi, preferisco rivedere il procedimento:

menu Statistics->endpoint List->IP4

cosi ho tutta la lista dei noti (da eliminare il broadcast)

MAC: guardo dentro i dati Ethernet dei pacchetti che riguardano i nodi

Porte: menu Statistics->endpoint List-> TCP ne ho trovate 13

la stessa cosa con UDP ne ho trovate 2

mi complico la vita? esiste un metodo piu veloce?

2. Quali sono le richieste scambiate con browser e quali sono i numeri dei pacchetti coinvolti.

Quali sono gli URI degli ggetti scambiati.

Risposta:

filtrando protocollo HTTP trovo due GET (pacchetti 1 e 9) due risposte (pacchetti 8 e 11)

l'URI lo trovo sugli header del protocollo HTTP, la voce è del tipo

Full request URI: http://10.10.10.10:8080/index.php

a. in risposta il server restituisce un file in che linguaggio è scritto il file?

javascript ..

b. nel file viene costruito un array, quanto è lungo e che etichetta ha:

il file è di 1300 elementi

etichetta COMMET

c. che valori hanno i suoi elementi?

valori "vEl", tutti gli elementi hanno lo stesso valore

3. Nel pacchetto n.17 si sa che il server restituisce al client un malware: sai dire quando inizia la conversazione client-server e che tipo di programma viene inviato

Risposta

inzio conversazione pacchetto 13.

una dll ???

1) Va bene come hai fatto

2) Ok per l'identificazione dei flussi HTTP
a) Per essere precisi, il file è html che contiene anche del codice Javascript
b) Array: "qSNgVk..." (1300 elementi). Per quanto riguarda l'"etichetta", se intende i "Javascript labeled statement" non ne vedo.. altrimenti non ho capito cosa chiede :-)
c) "qSNgVk..." contiene elementi di tipo "Element Node" con nome nodo "COMMENT" e data "vEl".

3) Inizio: pkt 13.
Il tipo di programma è "Windows (PE format) executable". Si capisce dal messaggio "This program cannot be run in DOS mode" che tutti i file di questo tipo hanno.

2) La seconda richiesta GET è verso l'uri "http://10.10.10.10:8080/index.phpmfKSxSANkeTeNrah.gif" e si riceve come risposta un oggetto di tipo "image/gif"

3) Potresti avere un NIDS che ti segnala del traffico sospetto. Oppure potresti accorgerti guardando manualmente il contenuto del traffico.. in questo caso servirebbe una tua conoscenza a priori del comportamento del malware..

21/04/2017

Esaminando il traffico reso disponibile alla pagina: https://homes.di.unimi.it/cimato/SSR/esame/ rispondere alle domande nello spazio predisposto.

1. Conversazione sicura (stream 4)
    a. Quali nodi IP sono sorgente o destinazione di traffico in una conversazione cifrata? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti? Quale protocollo stanno usando

    b. Quali cifrari sono offerti al server per proteggere la conversazione?

    c. Quale cifrario viene scelto per la connessione?

2. Traccia DNS
    a. Quale host sta generando nelle query errori DNS

    b. In quali altri conversazioni lo stesso nodo è coinvolto?

3. In un'altra conversazione cifrata (stream 8) a quale server il client cerca di connettersi?

1.Conversazione sicura (stream 4)

a. Quali nodi IP sono sorgente o destinazione di traffico in una conversazione cifrata? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti? Quale protocollo stanno usando

Applicando il filtro "tcp.stream eq 4" possiamo osservare i pacchetti relativi alla conversazione sicura richiesta

Il client è 192.168.1.71, porta 57060, MAC d4:3d:7e:a6:41:fd
Il server è 52.202.146.168, porta 443, MAC 38:3b:c8:ee:ea:29
Per instaurare la conversazione sicura stanno usando il protocollo TLS v1.2

b. Quali cifrari sono offerti al server per proteggere la conversazione?
Dal pacchetto 131, il "client hello", notiamo che il client propone al server ben 26 cipher suites:

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)

Domanda: all'esame andrebbe bene indicare solo i codici finali? per evitare errori di scrittura e risparmiare tempo...

c. Quale cifrario viene scelto per la connessione?
Nel pacchetto 136, il "server hello", il server sceglie la cipher suite 0xc02f ovvero:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Domanda: la seguente stringa si legge: RSA con AES a 128 bit e SHA256?

2. Traccia DNS
a. Quale host sta generando nelle query errori DNS
192.168.1.71

b.In quali altri conversazioni lo stesso nodo è coinvolto?
immettendo il filro :
ip.src==192.168.1.71 and !dns scopriamo in quali altri conversazioni il nodo è coinvolto, di seguito i protocolli utilizzati con le relative destinazioni:
IGMPv3 con 224.0.0.22
TLSv1.2 con 52.1.241.62
TLSv1.2 con 162.125.17.3
TLSv1.2 con 204.79.197.200
NBNS con 192.168.1.255
LLMNR con 224.0.0.252
TLSv1.2 con 52.202.146.168
TLSv1.2 con 52.7.228.130
TLSv1.2 con 52.0.227.230
TLSv1.2 con 52.0.77.117
TLSv1.2 con 204.79.197.200
TLSv1.2 con 66.151.158.177

3. In un'altra conversazione cifrata (stream 8) a quale server il client cerca di connettersi?

52.202.146.168

1 - conversazione sicura

b) direi di si.. una volta che indichi quanti sono e il pacchetto che li contiene, puoi indicare semplicemente i codici se sei stretto con i tempi..

c) si!

2 - traccia DNS

b) ok, io filtrerei anche per "ip.dst==192.168.1.71" (poi unirei i risultati) visto che la domanda dice solo "conversazioni" senza specificare se come sorgente o destinazione..

21/06/2017

19. Quali nodi sono coinvolti nel traffico?

.....
.....
.....
.....

20. Quali nodi effettuano richieste ARP?

.....

21. Quale nodo fornisce il servizio HTTP?

.....

22. In una conversazione HTTP vengono scambiate 2 password. Quali sono?

19)Quali nodi sono coinvolti nel traffico?

Distinguiamo
nodi sorgenti:
159.149.152.12
159.149.152.9
178.63.37.166

Nodi destinatari
159.149.152.12
159.149.152.255
178.63.37.166

20)Quali nodi effettuano richieste ARP?
Il nodo che fa la richiesta ARP è il 159.149.152.254 con MAC Enterasy_5c:4d:e0

21)Quale nodo fornisce il servizio HTTP?
178.63.37.166

22)In una conversazione HTTP vengono scambiate due password. Quali sono?
In modalità post vengono fornite le credenziali identificate da:
Nome campo = pass
Valore = alamakota

L'altra pass che viene scambiata è: a290bWFwc2E seguita dai caratteri \n\r

Ok, risposte quasi corrette..

Due precisazioni:

Le password scambiate sono: "alamakota" e "a290bWFwc2E="

Esaminando il traffico reso disponibile alla pagina: https://homes.di.unimi.it/cimato/SSR/esame/ rispondere alle domande nello spazio predisposto.

1. Conversazione FTP
   a. Quali nodi IP sono sorgente o destinazione di traffico in un trasferimento di file con FTP? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

   b. Quale file si sta tentando di trasferire?

   c. Quando avviene (se avviene) il trasferimento (indicare il nr del messaggio di risposta)?

   d. Quale è la sequenza di comandi ftp?

   e. Quali sono l'account e la password utilizzati?

   f. Individuare i messaggi di reset inviati

   g. Indicare altri protocolli usati nella collezione di pacchetti fornita

a. Quali nodi IP sono sorgente o destinazione di traffico in un trasferimento di file con FTP? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

192.168.75.1 00:50:56:c0:00:08
192.168.75.132 00:0c:29:0f:71:a3

Porte: 21, poi tutte le porte tra 1046 e 1058, 3655,3656,3658,3668,3669,3670,3671,3672,3673,3674,3675,3676,3677,3686

La domanda non richiede solo le porte utilizzate nel protocollo applicativo FTP?

Se filtriamo il file per protocol=FTP le uniche porte coinvolte sono la 21 e la 3655.

b. Quale file si sta tentando di trasferire?

db1.csv

c. Quando avviene (se avviene) il trasferimento (indicare il nr del messaggio di risposta)?

Il trasfermiento del file db1.csv non avviene mai!

d. Quale è la sequenza di comandi ftp?

USER, PASS, SYST, PWD, PASV,LIST,CWD,PASV,LIST,PWD,TYPE,PASV,STORE,PASV ,LIST,TYPE,PASV,STOR,PASV,LIST,TYPE,PASV,STORE,PASV,LIST,TYPE,PASV,STORE ,PASV,LIST,TYPE,PASV,STORE,PASV,LIST,PASV,LIST

e. Quali sono l'account e la password utilizzati?

user: Administrator
pass: napier

f. Individuare i messaggi di reset inviati

62,88,113,138,164

g. Indicare altri protocolli usati nella collezione di pacchetti fornita

ARP,DNS

Salve a tutti

volevo rispondere in merito a certe domande

c. Quando avviene (se avviene) il trasferimento (indicare il nr del messaggio di risposta)?

Il trasfermiento del file db1.csv non avviene mai!

non riesco a capire come verificare se il trasferimento è andato a buon fine. Noto però più volte "Access denied" subito dopo la richiesta del file

g. Indicare altri protocolli usati nella collezione di pacchetti fornita

ARP,DNS

Non ho trovato paccheti DNS, ma LLMNR.
considero quest'ultimo come DNS, cioè non lo indico come LLMNR?

Permalink | Visualizza intervento genitore

Re: Esame 21/06/2017 - esercizio wireshark
di matteo camilli - Friday, 19 January 2018, 14:50

- Il trasferimento non avviene mai (proprio perchè l'accesso viene sempre negato).

- LLMNR è praticamente un DNS nella rete locale.. come risposta andrebbe bene anche LLMNR.

Permalink | Visualizza intervento genitore

Re: Esame 21/06/2017 - esercizio wireshark
di vincenzopaolo diperna - Saturday, 20 January 2018, 10:45

per quanto riguarda il trasferimento, per esempio, come troverei allora se fosse andato a buon fine?

Permalink | Visualizza intervento genitore

Re: Esame 21/06/2017 - esercizio wireshark
di matteo camilli - Monday, 22 January 2018, 12:33

Dipende da cosa succede..

i messaggi positivi cono quelli nella serie 200 (es., `250`="Requested file action okay, completed.")..

se ti interessa puoi dare un'occhiata qui trovi tutti i codici associati ai messaggi: https://en.wikipedia.org/wiki/List_of_FTP_server_return_codes

17/07/2017

Esaminando il traffico reso disponibile alla pagina: https://homes.di.unimi.it/cimato/SSR/esame/ rispondere alle domande nello spazio predisposto.

1. Conversazione SMTP
    a. Quali nodi IP sono sorgente o destinazione di traffico in un trasferimento di file con SMT? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

    b. Quali sono mittente e destinatario del messaggio?

    c. Quale è la sequenza di comandi SMTP?

    d. Quali sono i software utilizzati (mail server/client, etc)?

1

a

Client
IP 192.168.0.12
MAC 00:0c:29:6a:94:c5
Porta 1713

Server
IP 192.168.0.13
MAC 00:0c:29:0f:71:a3
Porta 25

b

mittente Fred Smith martin.tor@4salet.com
destinatario bert.manly@five8nine.com

c
1 S:220 napier Microsoft ESMTP ...
2 C: EHLO napier
3 S: 250 napier Hello 192.168..0.12 ...
4 C: MAIL FROM ...
4 S: 250 ...
5 C: RCPT TO ...
6 S:250
7 C: DATA
8 S:354
9 C: DATA fragment (il client avvisa il server che i dati saranno riassemblati al frame 15)
10 C invia la mail con protocollo IMF
11 S:250
12 C QUIT
13 S: 221

d

Server: Microsoft Exchange versione 6 con ESMTP

Client: Microsoft Outlook Express 6.0 come notiamo nel campo X-Mailer del pacchetto 15, pacchetto in cui viene inviata la mail

12/01/2018

Esaminando il traffico reso disponibile alla pagina: https://homes.di.unimi.it/cimato/SSR/esame/
rispondere alle domande nello spazio predisposto.

1. Quali nodi IP sono sorgente o destinazione di traffico nella conversazione del primo pacchetto? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

2. Quali sono le richieste scambiate con browser e quali sono i numeri dei pacchetti coinvolti.

    a. Quali sono le caratteristiche del browser? Quali quelle del server?

    b. Qual è il nome del file scambiato e quanto è lungo in byte e quanti frame sono necessari?

    c. Cosa sta facendo probabilmente l'utente?

---

    d. Qual è il nome del dtd utilizzato nella pagina web?

3. Il client è coinvolto in altre due conversazioni, cosa sta facendo?

    a. Quali sono le associazioni fra IP e domini che puoi riportare?

    b. Quale server risponde?

1) Quali nodi IP sono sorgente o destinazione di traffico nella conversazione del primo pacchetto? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

L'IP del nodo sorgente è 145.254.160.237 con porta 3372 ed indirizzo MAC 00:00:01:00:00:00

L'IP del nodo di destinazione è 65.208.228.223 sulla porta 80 (http) e con MAC fe:ff:20:00:01:00

2) Quali sono le richieste scambiate con browser e quali sono i numeri dei pacchetti coinvolti.

Filtrando in base al protocollo HTTP ho trovato la seguente risposta:

Il client fa due richieste GET a due destinazioni con IP differenti che coinvolgono i pacchetti 4 (con risposta al pacchetto 38) e 18 (con risposta al pacchetto 27). La prima è la richiesta di un file mentre la seconda di una pagina web.

a. Quali sono le caratteristiche del browser? Quali quelle del server?

Il client risulta avere uno user-agent di tipo Mozilla/5.0 che lavora su Windows, mentre i due server che si possono trovare sono uno di tipo Apache e l'altro è un server CAFE/1.0.

(Ci sono altre caratteristiche da aggiungere?)

b. Qual è il nome del file scambiato e quanto è lungo in byte e quanti frame sono necessari?

Il file scambiato è download.html. Andando a cercare nella relativa risposta al frame 38 si può vedere che il segmento TCP ha una lunghezza totale di 18364 bytes ed è formato dall'assemblaggio di 14 frames.

c. Cosa sta facendo probabilmente l'utente?

In questo caso non sono molto sicuro su cosa debba basare la mia risposta. Forse con una delucidazione in più sarei in grado di capire a cosa ci si stia riferendo.

d. Qual è il nome del dtd utilizzato nella pagina web?

Andando ad analizzare la parte XML del pacchetto 38 si vede che viene specificato l'utilizzo di DTD/xhtml1-strict.dtd

3. Il client è coinvolto in altre due conversazioni, cosa sta facendo?

Oltre a quella riferita al primo pacchetto, la conversazione con 216.239.59.99 è ancora di tipo HTTP in cui si richiede la pagina web pagead, mentre quella con 145.253.2.203 è una richiesta di risoluzione DNS della pagina pagead2.googlesyndication.com.

a. Quali sono le associazioni fra IP e domini che puoi riportare?

b. Quale server risponde?

Queste ultime due domande mi hanno messo un po' in crisi, non saprei bene come comportarmi.

2c) direi che semplicemente ha richiesto la pagina "download.html" sul web server "www.ethereal.com" tramite browser Mozilla Firefox 5.0
3) c'è una risoluzione di un indirizzo tramite DNS e un'altra richiesta HTTP (server: pagead2.googlesyndication.com)

- a) dalla risoluzione della richiesta DNS si evince che il nome "pagead2.googlesyndication.com" è associato agli indirizzi (DNS record type A) "216.239.59.99" e "216.239.59.104"
- b) la successiva richiesta HTTP viene inviata a "216.239.59.99" che risponde a sua volta al client

Per il resto sono ok le risposte.

12/02/2019

Esaminando il traffico reso disponibile alla pagina: https://homes.di.unimi.it/cimato/SSR/esame/12feb/ rispondere alle domande nello spazio predisposto.

1. Quali nodi IP sono sorgente o destinazione di traffico nella conversazione HTTP? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

   a. Quali sono le richieste scambiate col server e quali file in download

   b. Quali sono le caratteristiche del client? Quali quelle del server?

---

2. Il file documenta una infezione. Quali sono il nome host e l'account coinvolti?

3. Uno dei file in download è uno script visual basic, dare i dettagli dello scambio

---

1. Quali nodi IP sono sorgente o destinazione di traffico nella conversazione HTTP? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

Il client è 172.16.2.96 con MAC 00:1C:23:9B:70:5E.

Il client fa diverse richieste GET a vari server. Quella della prima connessione è 187.33.238.74 con MAC 00:09:B6:BA:37:F1

La porta destinazione è la porta 80, quella sorgente varia da 49157 a 49212.

a. Quali sono le richieste scambiate col server e quali file in download

Vengono scambiare diverse richieste GET e vengono richiesti vari file, come: ncsi.tx; /bibi/w7.txt; /bibi/aw7.tiff; /bibi/w7.zip ..

--> Va bene indicare solo i file e non le pagine web? E' ok indicarne solo alcuni?

b. Quali sono le caratteristiche del client? Quali quelle del server?

Il client, esaminando la richiesta GET del pacchetto 117, ha uno User Agent: Mozilla/5.0 su Windows NT 6.1

Il server 65.181.225.20 esaminando la risposta HTTP del pacchetto 119 è Apache/2.2.22

2. Il file documenta una infezione. Quali sono il nome host e l'account coinvolti?

Dal pacchetto 484 si rileva un'infezione con Host: ww.denyatinskiy.ru ed il nome dell'account è FROGGY-PC-Matthew-Frogman.

--> E' corretto?

3. Uno dei file in download è uno script visual basic, dare i dettagli dello scambio

--> Dove trovo lo script VBA? Trovo solo immagini, file html ed applicazioni Javascript

---

Quali nodi IP sono sorgente o destinazione di traffico nella conversazione HTTP? quali porte sono coinvolte? Qual è il MAC dei dispositivi coinvolti?

- Qui io filtrerei il traffico in base al protocollo http e andrei semplicemente a vedere gli endpoint delle comunicazioni.

Quali sono le richieste scambiate col server e quali file in download

- Risponderei mettendo l'elenco delle richieste specifiche effettuate contenente l'url per cui è stata fatta la richiesta e il riferimento (id) ai pacchetti coinvolti. Per ogni richiesta individuata scriverei il file che viene scaricato.

Quali sono le caratteristiche del client? Quali quelle del server?

- Ok come hai scritto.

Il file documenta una infezione. Quali sono il nome host e l'account coinvolti?

- Qui devi vedere il contenuto della comunicazione usando l'opzione "follow tcp stream". Visto che i dati sono in chiaro non ci sono problemi a trovare cose anomale (come credo tu abbia fatto).

Uno dei file in download è uno script visual basic, dare i dettagli dello scambio

- Qui dovrei vedere il file. Non trovi nessun file con estensione .vb?

---

scan.pcap

Scan

19 - Quali nodi sono coinvolti nel traffico?

10.0.2.2
10.0.2.3
10.0.2.15
159.149.152.13

20 - Quale nodo fornisce il servizio DNS?

10.0.2.3 (Righe 7,8)

21 - Quale nodo fornisce il servizio DHCP?

10.0.2.2 (Righe 1-4)

22 - Identificare eventuali attività sospette?

Il PC con IP 10.0.2.15 fa un Xmas scan verso l'IP 159.149.152.13 e trova la porta 443 aperta

23 - Scrivere una regola iptable che permetta di registrare il traffico sospetto individuato.

iptables -A INPUT --p tcp --tcp-flags ALL FIN,PSH,URG -j LOG

Le attività sospette sono:

SYN scan, Ack scan, XMAS dal nodo 10.0.2.15 verso il nodo 159.149.152.13.

Questo è sufficiente a rispondere alla domanda fatta..

telnet.pcap

19. Quali nodi sono coinvolti nel traffico?
Source:
172.16.175.1
172.16.175.129
172.16.175.2

Destination
172.16.175.1
172.16.175.129
172.16.175.2
172.16.175.255 indirizzo di broadcast della rete

20. Quale nodo fornisce il servizio DNS?
172.16.175.2

21. Quale nodo fornisce il servizio Telnet?
172.16.175.129

22. Identificare le credenziali per accedere alla macchina che fornisce il servizio Telnet
Le credenziali corrette sono le seguenti:
debian login: cchhuuppaa
Password: grepmylollipop

Tra i nodi del traffico non includere quello che termina con .255 in quanto è un indirizzo broadcast (come giustamente hai specificato).

Il login non è "cchhuuppaa", ma "chupa".. se osservi bene il server reinvia ogni carattere ricevuto al client.
Lo vedi dal colore diverso (blu/rosso) di ogni carattere nel TCP flow.

Il resto è Ok!