SOLUZIONE: Hacking This Site – Application – Application Challenge 2

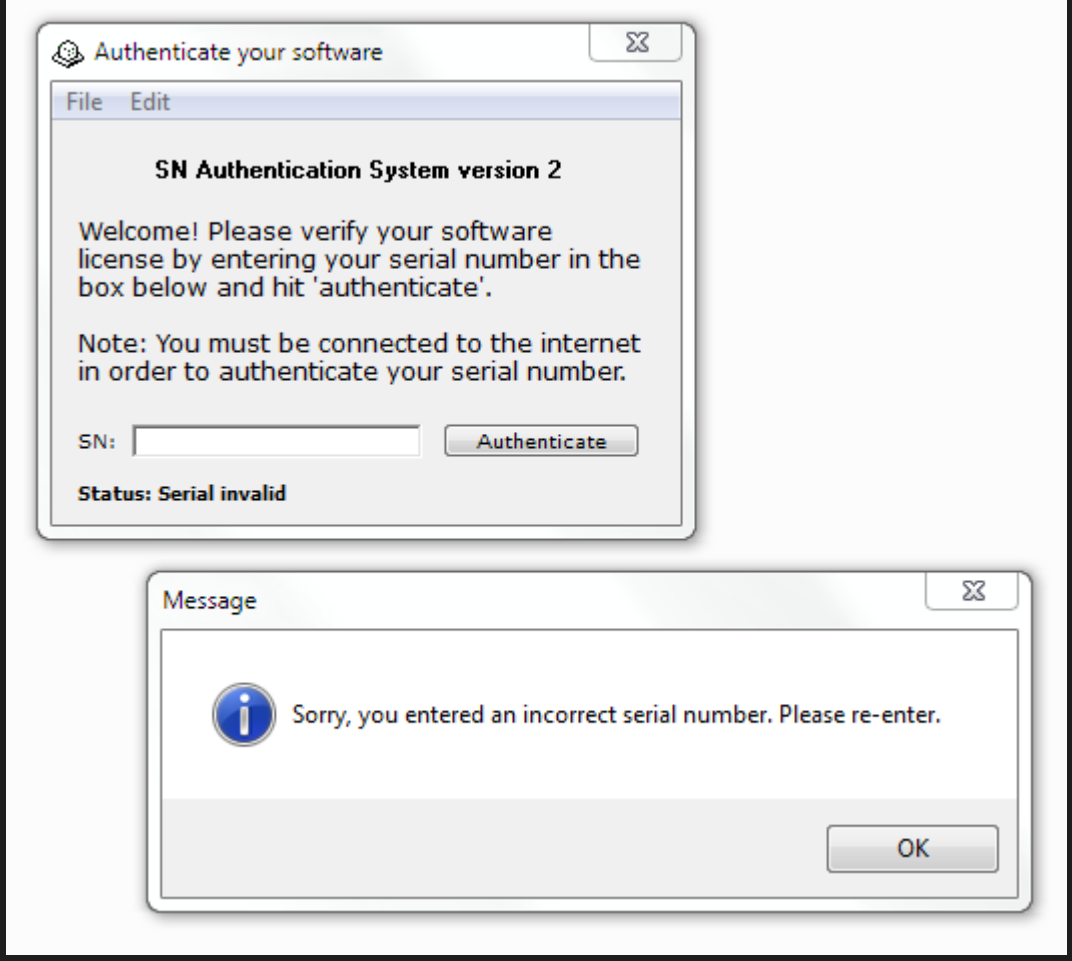
aprile 18th, 2023

Da diversi anni, cerco di avvicinarmi all'apprendimento delle procedure di cracking dei programmi, a tal punto che per un periodo mi sono messo anche a programmare in Assembly, affascinato dalla visione dei dump esadecimali.
Purtroppo devo studiare ancora molto, in quanto è molto complicato riuscire a crakkare un software. Giusto per avere un assaggio, vi rimando al mio articolo Come crakkare un videogioco. Si tratta di una mia conquista in ambito informatico, di cui ne vado molto fiero grazie alla sua complessità.
Ieri, sul sito Hack This Site, ho trovato nella categoria Application, una serie di software che possono essere crakkati. Solitamente sono conosciuti come CRACK ME. Come si intuisce dal nome, sono dei software che consentono di mettersi in gioco, di capire dove uno può arrivare, di prendere consapevolezza di quanto uno sia esperto nel campo del cracking.
Ho deciso di scaricare diverse applicazioni, ma sono rimasto più affascinato dall'Application Challenge 2. Si tratta di una rappresentazione fedele del classico programma che richiede un codice di licenza.
Dopo aver fatto alcune prove, ho deciso di cercare su internet la soluzione. Ne sono riuscite a trovare diverse.
Questo mi ha fatto ritornare alla mente una valutazione che avevo già fatto anni fa. Non è importante come crakki il software, ma se lo riesci a crakkare oppure no. Come per tutti i problemi, esistono differenti soluzioni. Una

vasca da bagno può essere svuotata con un cucchiaio, con un secchio, con una pompa idraulica, o semplicemente aprendo il tappo dello scarico.
Risulta interessante come diverse persone, di fronte allo stesso problema, reagiscono in modo diverso. Risulta poi chiaro comprendere chi è quello più sveglio di tutti. Ad ogni modo, andare a cercare una soluzione già pronta, in alcuni casi potrebbe essere un modo per apprendere sempre di più. Il confronto con gente che ne sa più di noi in un certo campo, è sempre utile. Possiamo usare i confronti per imparare sempre qualcosa di nuovo, così nell'informatica, come nella vita.
Io ieri mi sono fatto da parte, ho capito che non avevo ancora le conoscenze per poter crakkare quel software, così ho deciso di confrontarmi con chi ne sapeva più di me. Vi parlerò della soluzione che mi ha colpito di più.
Chissà, magari confronto dopo confronto imparerò a crakkare diversi software.
Per il momento mi rimbocco le maniche ed inizio da questo.
Dall'Application Challenge 2.

Application Challenge 2

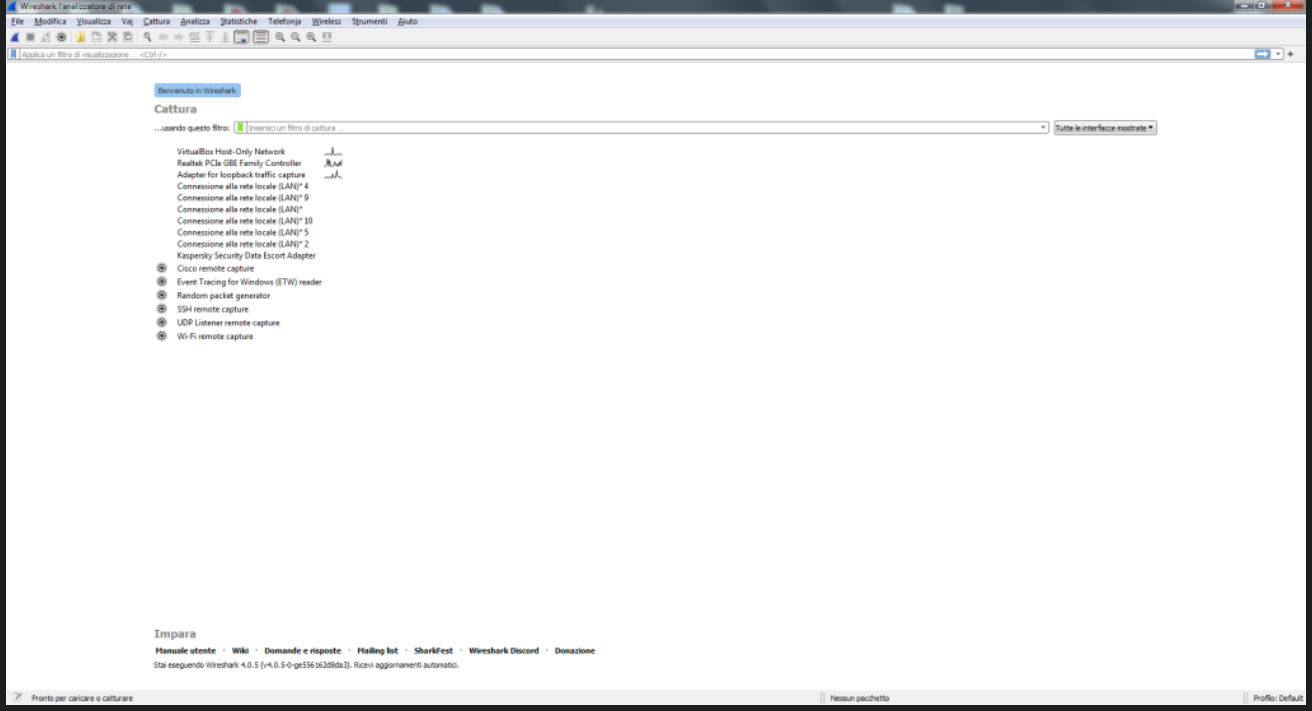
Come vi avevo anticipato e come potete notare, si presenta come il classico programma che richiede un product key.
"Benvenuto! Per favore verifica la tua licenza software inserendo il product key nel campo sottostante e fai click su 'Authenticate'.
Nota: Devi essere connesso ad internet per autenticare il tuo product key."
Se provo a fare click sul pulsante "Authenticate" senza digitare alcun product key, mi compare il seguente avviso.



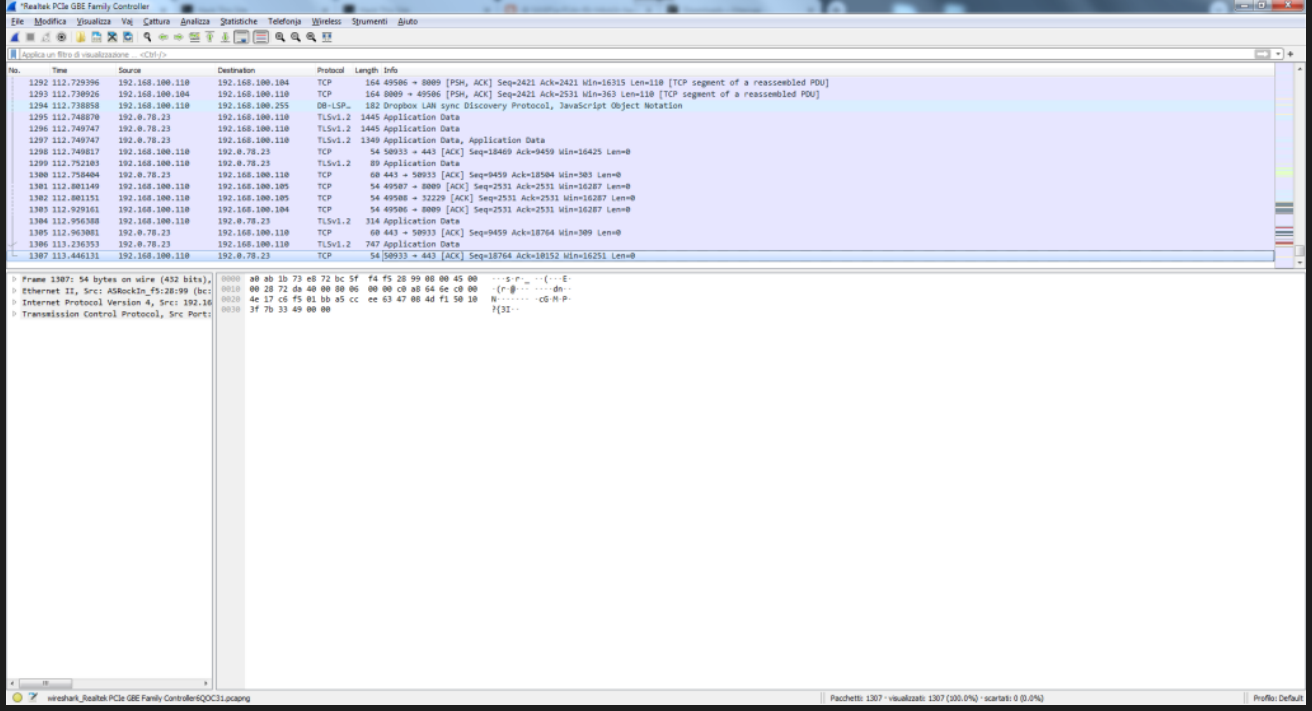
Ogni tanto, inserendo un product key di prova, si può notare la scritta "Connecting...", forse dovuto ad un piccolo ritardo nella trasmissione dei dati da parte dell'applicazione.

Quella che vi sto per illustrare, è la soluzione di sp@root.
In un suo articolo, Hack This Site! – Application 2, per ricollegarmi a quanto già scritto, l'autore spiega che per crakkare un software si può manipolare il sistema operativo, il software, oppure utilizzare altri sistemi per raggiungere lo scopo.
Fa inoltre notare che è il programma stesso, a dire che bisogna essere collegati ad internet per eseguire una verifica del product key immesso.

Lo possiamo capire anche dall'immagine che vi ho mostrato prima.
Purtroppo ieri, non ci avevo pensato.
sp@root propone di andare a sniffare il traffico di rete alla ricerca dei dati trasmessi dal software che dobbiamo crakkare.
Ma cosa significa sniffare il traffico di rete?
Specialmente negli ultimi anni, sono sempre di più i programmi che trasmettono e ricevono dati su internet. Questi dati, possono essere intercettati e letti alla ricerca di varie informazioni. In questo modo è possibile capire cosa sta succedendo in background.
Un software che ci permette di fare questo è Wireshark.
Si tratta di un software che permette di analizzare un protocollo, funge da packet sniffer per sniffare i pacchetti che vengono inviati e ricevuti all'interno di una rete, permette di risolvere problemi di rete e analizzare quest'ultima ed è utile anche per lo sviluppo di protocolli, di software per la comunicazione e per la didattica. Naturalmente anche per il debug delle comunicazioni di rete da parte dei software.
Wireshark permette di sniffare il traffico di moltissime schede di rete presenti sul computer in cui viene eseguito. Per farlo utilizza WinPcap e quando ne viene proposta l'implementazione durante l'installazione di Wireshark, è importante acconsentire.
WinPcap viene utilizzato da diversi packet sniffer e risulta fondamentale per accedere alla funzionalità principali di questi, ossia sniffare i pacchetti in rete.
Ritorniamo al crack del software.
Dopo aver installato Wireshark in modo completo, integrando anche WinPcap, apriamolo.



Selezioniamo la scheda di rete di nostro interesse.
Io ho selezionato la scheda di rete ethernet “Realtek PCIe GBE Family Controller”, in quanto rappresenta la scheda di rete ethernet che mi ha collegato ad Internet e sulla quale sto attualmente lavorando.
Fate doppio click o click con il tasto destro sopra la voce relativa alla scheda di rete che intendete monitorare. Se fate click con il tasto destro si aprirà un menu. Selezionate “Avvia la cattura”.
Wireshark inizierà a sniffare il traffico di rete.
Adesso andiamo ad eseguire Application Challenge 2, ossia il software che vogliamo crakkare.
Digitiamo “TEST” nel campo in cui dovremmo digitare il product key, proprio come abbiamo fatto prima.
Application Challenge 2 cercherà di verificare il nostro product key collegandosi ad internet e scambiando dati con l’esterno.
L’immissione di un product key di prova, è fondamentale per far avviare almeno una trasmissione di dati.
Quindi andiamo a stoppare la cattura dei pacchetti, cliccando sul quadrato di colore rosso posto in alto a sinistra dell’interfaccia grafica di Wireshark.
Adesso avremmo di fronte a noi tutta la lista dei pacchetti catturati.



Sopra questi pacchetti troveremo un campo che assomiglia alla barra degli indirizzi del nostro web browser. Questo campo riporta la scritta “Applica un filtro di visualizzazione …”

In questo campo di testo, digitiamo “http.request”.

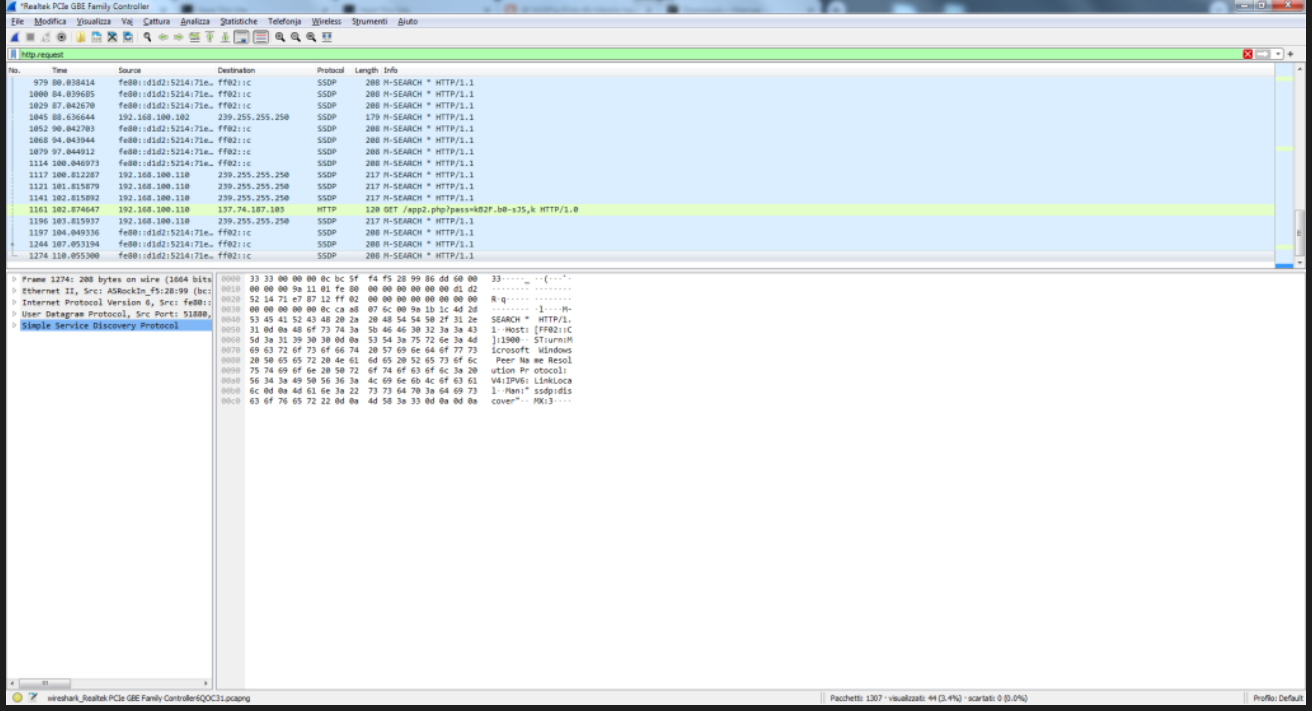
Questo campo ci consente di filtrare tutti i pacchetti di rete catturati, in modo tale che possiamo escludere tutti quelli che non ci interessano e rendere più semplice l’analisi.

Dopo aver digitato “http.request” facciamo click sulla freccia blu presente sempre alla destra del campo dei filtri, per poter eseguire il filtraggio e visualizzare solo i pacchetti di nostro interesse. Ossia “http.request” che non sono altro che le richieste eseguite tramite protocollo HTTP.

Subito dopo avremmo di fronte a noi una lista molto più semplice da leggere. Con meno elementi rispetto a quanti ne avevamo prima.

Potremmo inoltre vedere i metodi di trasmissione tipo GET o POST.

Come noterete ci sono alcuni record di colore verde in quanto Wireshark mette in risalto alcuni pacchetti, diciamo quelli più interessanti.



Se notate, abbiamo catturato il pacchetto seguente.

```
1161    102.874647      192.168.100.110 137.74.187.103  HTTP    120
GET /app2.php?pass=kB2F.b0-sJS,k HTTP/1.0
```

Nel mio caso si tratta del pacchetto numero 1161. Vuol dire che Wireshark ne ha catturati altri 1160 prima di questo.
Il pacchetto è stato trasmesso dal mio computer con ip 192.168.100.110 ad un altro computer con ip 137.74.187.103.
Apriamo il Prompt dei comandi ed eseguiamo il comando seguente che consente di fare un'interrogazione al server DNS di Google che risponde all'ip 8.8.8.8

```
nslookup 137.74.187.103 8.8.8.8
```

Il server DNS di Google ci ha risposto che l'hostname dell'ip 137.74.187.103 è hackthissite.org
Basterà infatti digitare nella barra degli indirizzi del web browser 137.74.187.103 per visualizzare il sito Hack This Site.

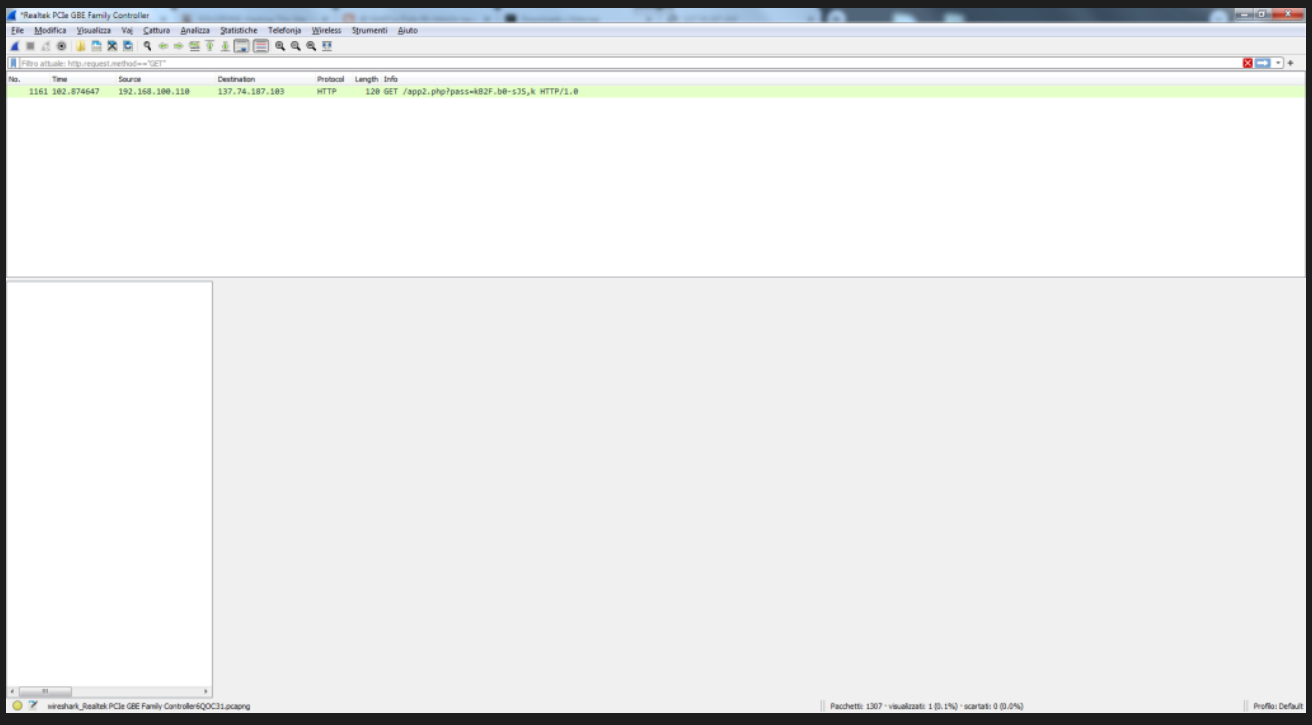
```
Server:  dns.google
Address:  8.8.8.8
```

```
Nome:    hackthissite.org
Address:  137.74.187.103
```

In pratica Application Challenge 2 ha trasmesso dei dati al server hackthissite.org
Adesso cerchiamo di studiare ancora di più il pacchetto catturato da Wireshark.
Notiamo che è stato utilizzato il protocollo di comunicazione HTTP e che il pacchetto è composto da 120 BYTE.
Il pacchetto è stato trasmesso con metodo GET.
Adesso andiamo a filtrare solo i pacchetti che usano il metodo di trasmissione GET andando a digitare nella barra dei filtri il comando seguente.

```
http.request.method=="GET"
```

Così facendo abbiamo tolto dalla visualizzazione moltissimi pacchetti.
Potremmo concentrarci solo sul pacchetto che sembra sia quello che stiamo cercando.
Avremmo potuto applicare questo filtro fin da subito, ma vorrei farvi comprendere meglio il funzionamento dell'applicazione.



Adesso ci stiamo avvicinando alla parte più interessante.

Facciamo click con il tasto destro sopra il pacchetto di nostro interesse.

Facciamo click su “Segui”.

Quindi facciamo click su “Flusso TCP”.

Verrà visualizzata la finestra seguente.

Di seguito vi riporto l’output in formato testuale.

```
GET /app2.php?pass=kB2F.b0-sJS,k HTTP/1.0
Host: appchall2.hts

HTTP/1.1 200 OK
Date: Mon, 17 Apr 2023 22:19:59 GMT
Upgrade: h2,h2c
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 299
Content-Type: text/html
Content-Language: en
Server: HackThisSite
Access-Control-Allow-Origin: *
Content-Security-Policy: child-src 'self' hackthissite.org
*.hackthissite.org htscdn.org *.htscdn.org discord.com; form-action
'self' hackthissite.org *.hackthissite.org htscdn.org *.htscdn.org;
upgrade-insecure-requests; report-uri https://hackthissite.report-
uri.com/r/d/csp/enforce
Referrer-Policy: origin-when-cross-origin
X-XSS-Protection: 0
Feature-Policy: fullscreen *
Public-Key-Pins-Report-Only: pin-
sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-
sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-
age=2592000; includeSubDomains; report-
uri="https://hackthissite.report-uri.com/r/d/hpkp/reportOnly"
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
Report-To: {"group":"default","max_age":31536000,"endpoints":
[{"url":"https://hackthissite.report-
uri.com/a/d/g"}],"include_subdomains":true}
NEL:
{"report_to":"default","max_age":31536000,"include_subdomains":true,"s
uccess_fraction":0.0,"failure_fraction":0.1}

63482-74819-88456-98378
45910-18394-85113-51290
10110-19101-59111-41563
11424-74719-19578-99238
25182-28381-85611-85258
62351-12939-12481-58020
63482-74819-88456-98378
45910-18394-85113-51290
```

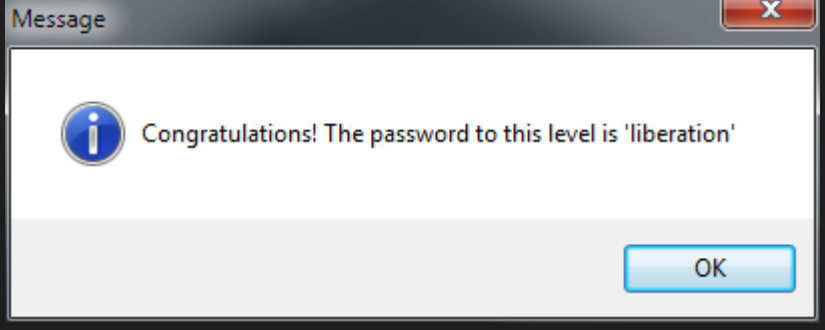
```
18381-21931-98680-86523

32910-21944-12391-51939
12389-16781-72893-71892
83478-91933-89823-98511
```

Direi che abbiamo fatto bingo! Cerchiamo però di capire qualcosa in più.
In questa finestra, in basso c'è scritto "1 pacchetto client, 2 pacchetti server, 1 turno."
Questo significa che noi, dal nostro computer e tramite Application Challenge 2, abbiamo inviato un pacchetto al server di Hack This Site che ci ha risposto con 2 pacchetti.
In questa finestra, i pacchetti inviati dal client, quindi da noi, sono evidenziati di rosso, quelli inviati dal server invece sono evidenziati in colore blu.
Sotto inoltre possiamo vedere tutti i product key accettati dal programma Application Challenge 2.

```
63482-74819-88456-98378
45910-18394-85113-51290
10110-19101-59111-41563
11424-74719-19578-99238
25182-28381-85611-85258
62351-12939-12481-58020
63482-74819-88456-98378
45910-18394-85113-51290
18381-21931-98680-86523
32910-21944-12391-51939
12389-16781-72893-71892
83478-91933-89823-98511
```

In pratica nel momento in cui immettiamo un product key, Application Challenge 2 invia un comando al server di Hack This Site che risponde con i product key riconosciuti come validi. In seguito Application Challenge 2 esegue un confronto con il product key che abbiamo immesso. Qualora sia presente fra quelli riconosciuti come validi, ci sarà mostrata la finestra seguente.



Adesso sappiamo quale è la password per passare al livello successivo.

```
liberation
```

Avete mai usato questa tecnica per crakkare un software?

Siete mai riusciti a guadagnarvi qualche accesso usando Wireshark?

Raccontatemi le vostre esperienze nei commenti.

aprile 18, 2023 Admin SOLUZIONI CRACKING

CRACKING, PASSWORD, REVERSE ENGINEERING, SNIFFING, SOLUZIONE

Rispondi

Scrivi qui il tuo commento...