Logo

Description automatically generated

SSL Stripping

Contents

[What is SSL Stripping? 2](#_Toc133332332)

[Tools used 2](#_Toc133332333)

[Results 3](#_Toc133332334)

[Conclusions 4](#_Toc133332335)

# What is SSL Stripping?

SSL stripping is exactly what it sounds like – stripping a secure connection and reducing it to an unencrypted connection. Doing this can allow any website to be vulnerable to different attacks and expose data that I would otherwise not be allowed to see. If successful, then this will leave the website vulnerable to different attacks such as HTTP method validation (see other report for details regarding that.) and more.

SSL stripping can be considered a Man in the middle attack, as it takes advantage of the TCP handshake which is always unencrypted traffic. By forcing the user into a connection which isn’t secure and encrypted allows attacks to steal passwords and other information that the user would assume is encrypted and confidential. Kiplin (2022)

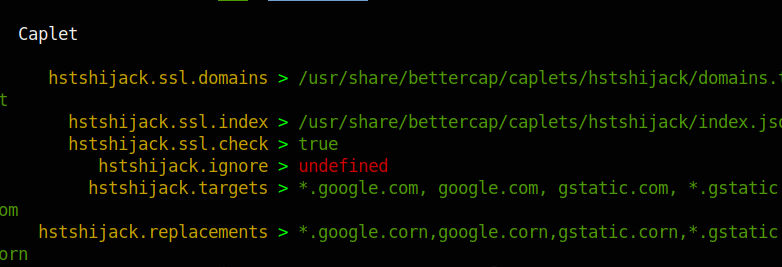
This attack takes advantage of people who aren’t paying attention and although it is simple it can be devastating if a user were to fall for this kind of attack and have their credit card information leaked.

# Tools used

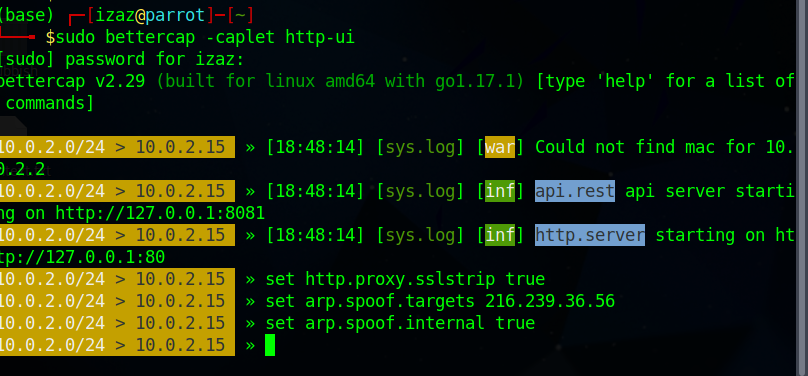
ParrotOS (Any OS can be used in its place)

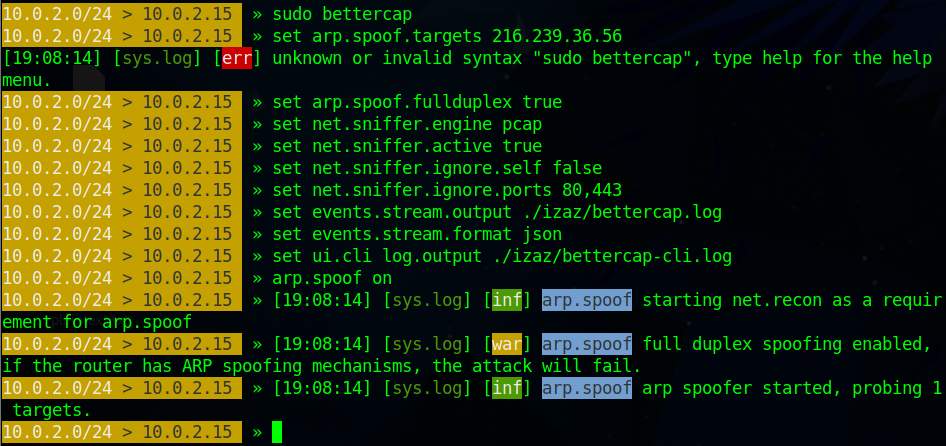
Bettercap

Firefox/Chromium

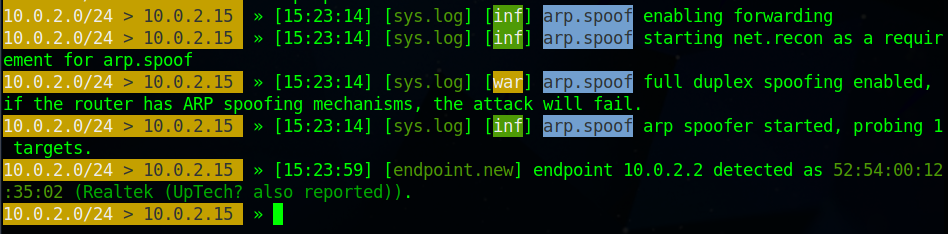


Using the caplet in bettercap will spoof the dns, doing this can allow for hackers to bypass the encryption and possibly attack users. As we can see above instead of using google.com for the DNS it switches the traffic to have google.corn





Above is the screenshots of the many different configurations and settings that can be applied to bettercap. These settings allowed me to monitor traffic and only everything that was unencrypted would then get passed onto the log specified above.



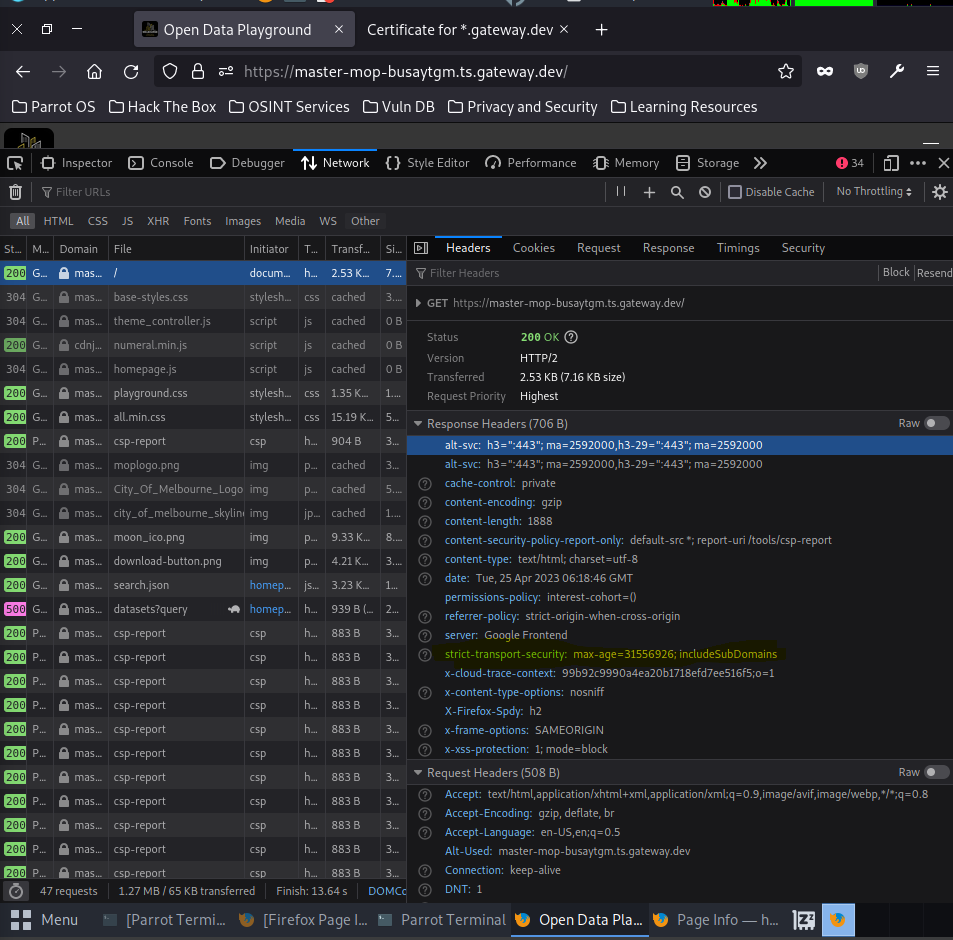
It seems like the only connection that can be found is my Vm’s Mac Address, it doesn’t seem to log any information regarding the MOP website or any other traffic I try to capture.

# Results

There might need to be more research into using bettercap but this may be a dead end due to HSTS.

HSTS is a method that prevents SSL stripping. If this roughly 7-10 years ago this attack may have worked but since HSTS became popular in roughly 2017 and HTTPS was forced to become a minimum of security requirements. Security (2017)

You can see that HSTS is enabled within the website by simply using a proxy and trying to access the website, by doing this the proxy would attempt to force a HTTP connection and that where HSTS interrupts and forces you to either obtain a certificate (which can be self-generated but then still makes you use HSTS) or to go back.



In the section that’s highlighted in yellow we can see that there is a strict transport security proving that this website does have HSTS and thus trying to force HTTP is pointless as the whole purpose of HSTS is to prevent this type of attack

# Conclusions

* Research more modern attacks
* Attacks that were prevalent years ago may not be as strong as what they once were.
* Use tools that are simple and intuitive