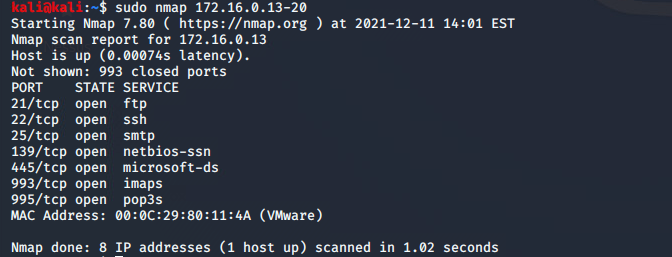
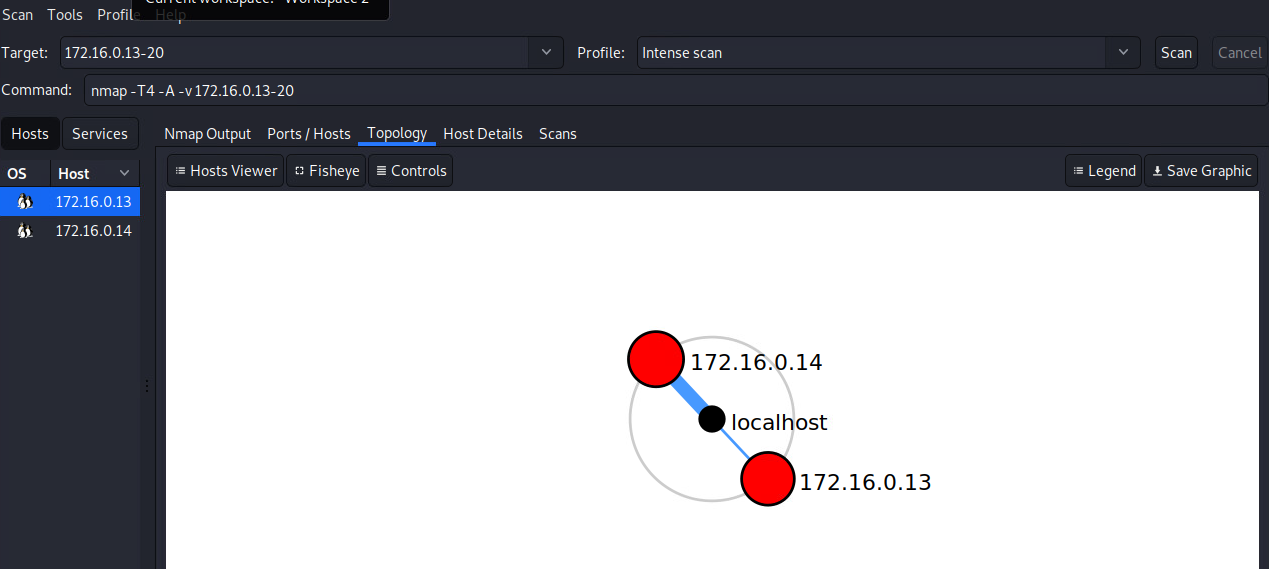
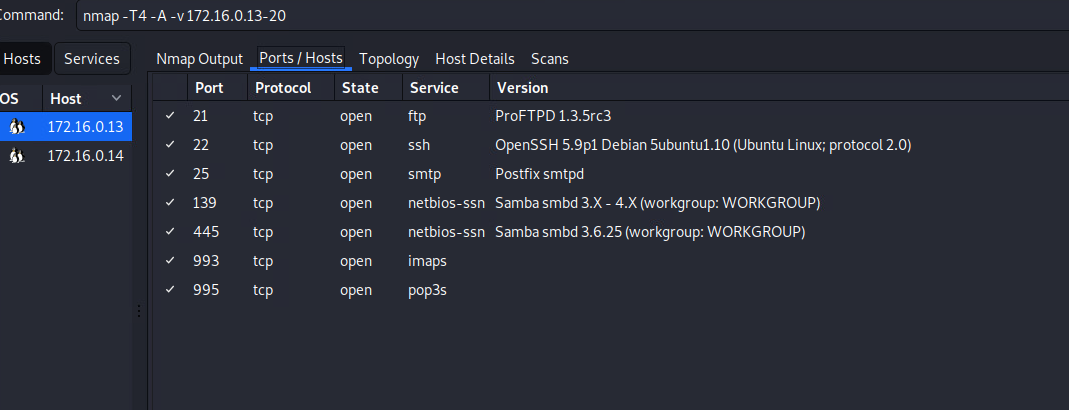
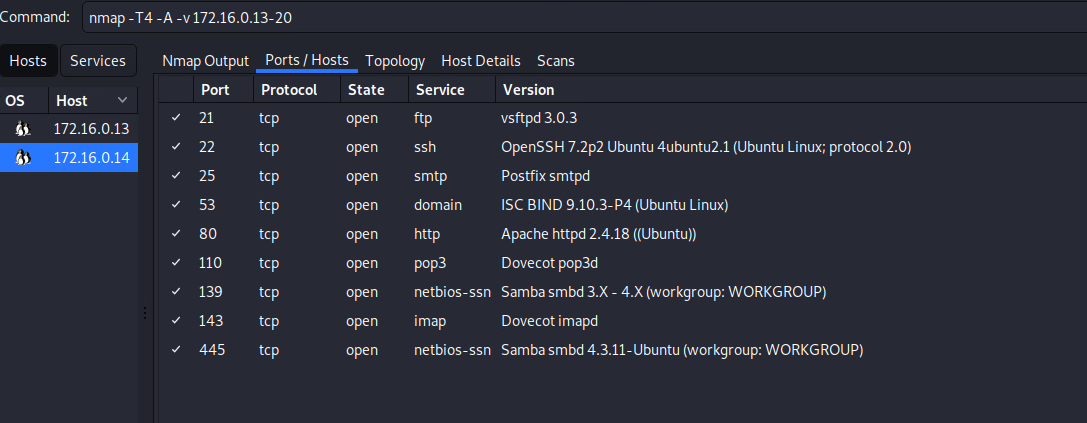
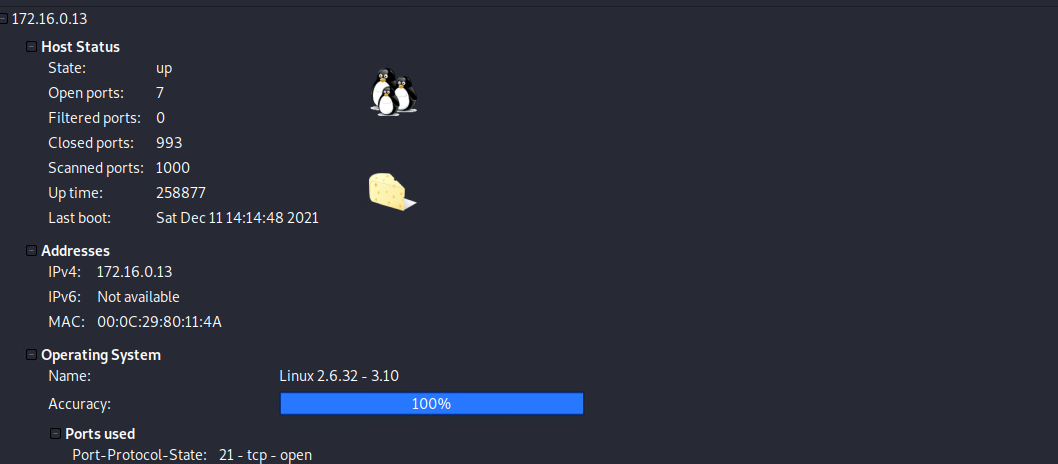
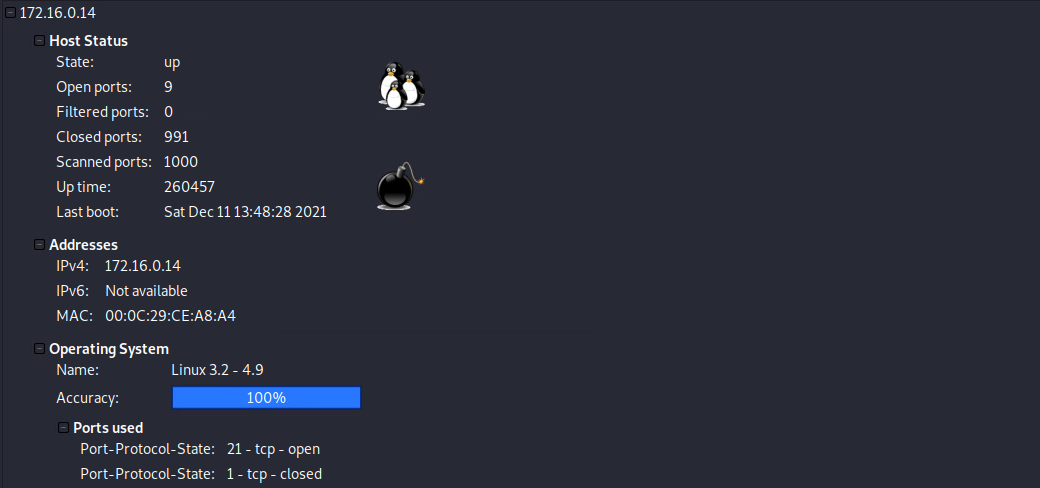
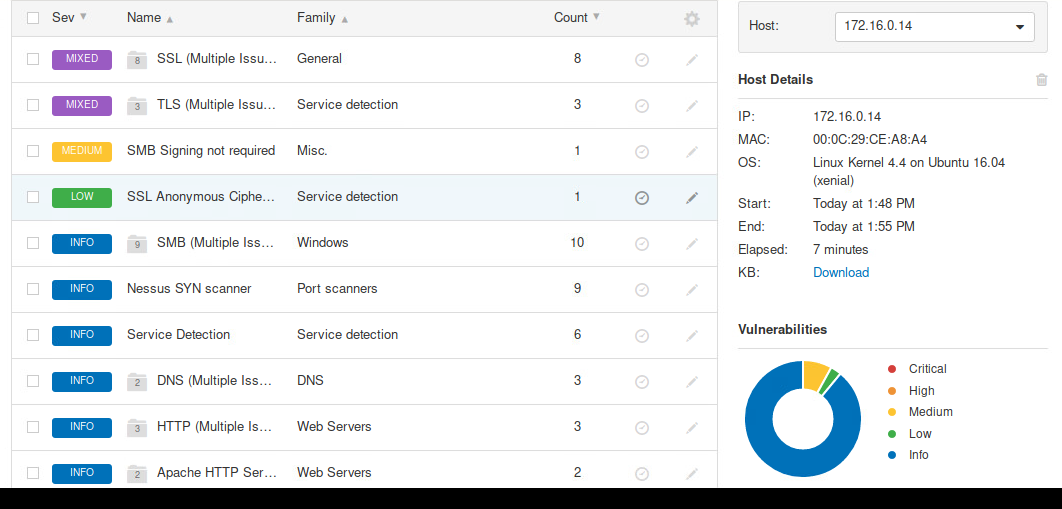
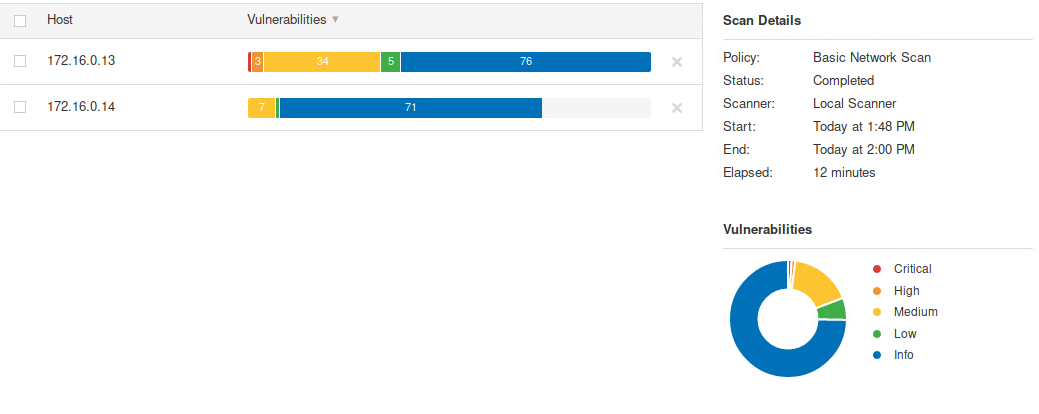
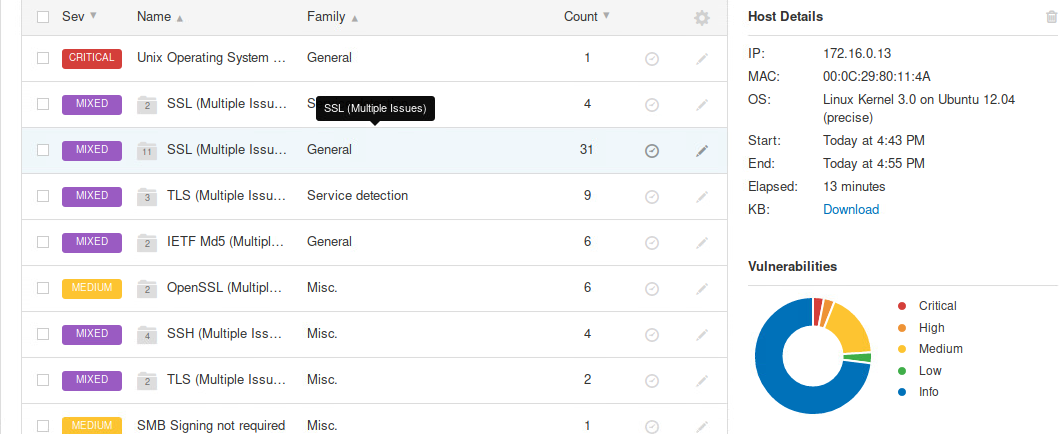
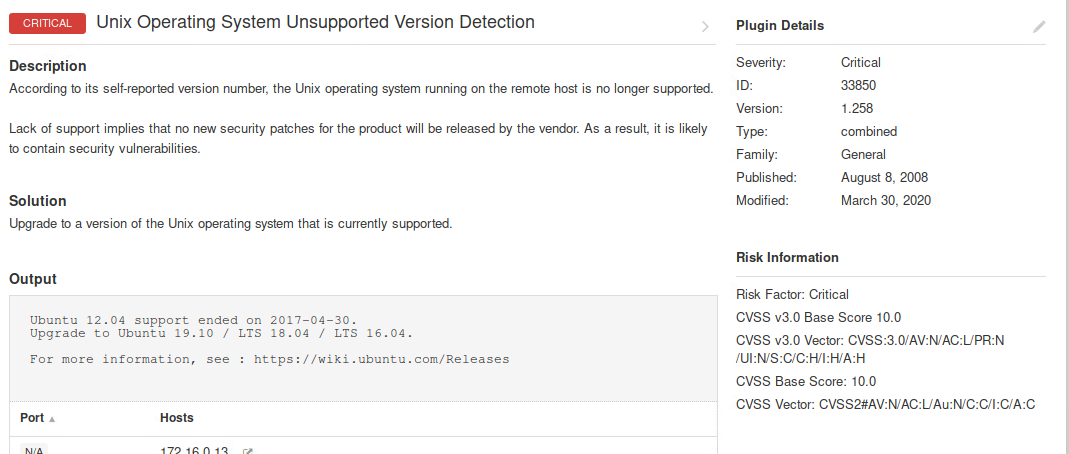
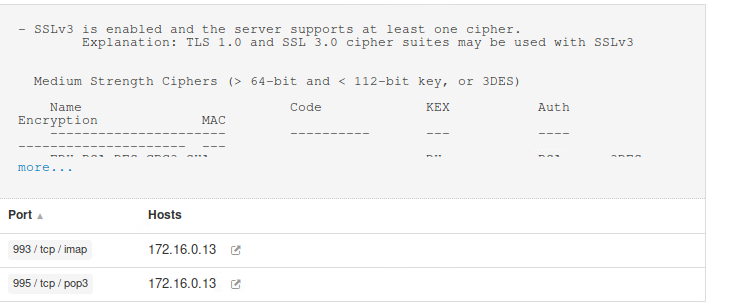
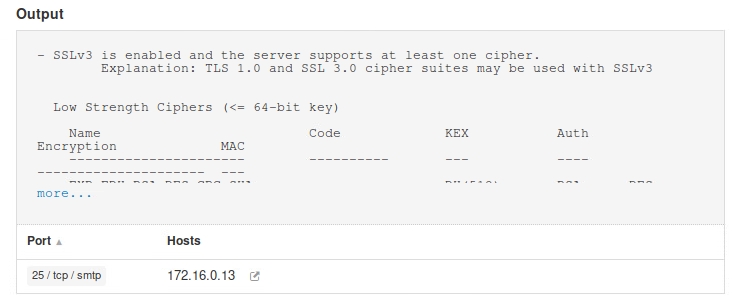
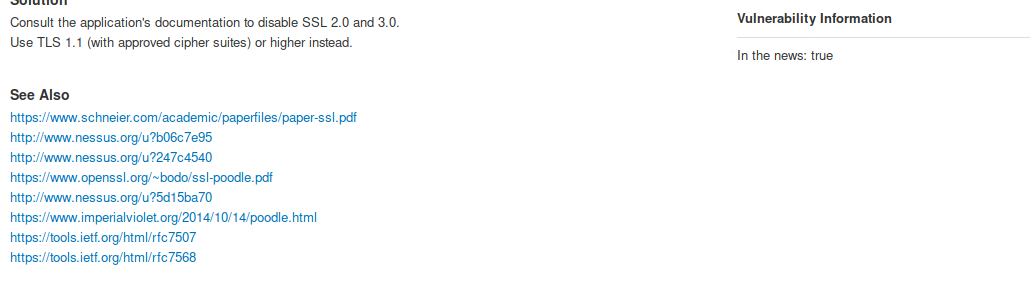
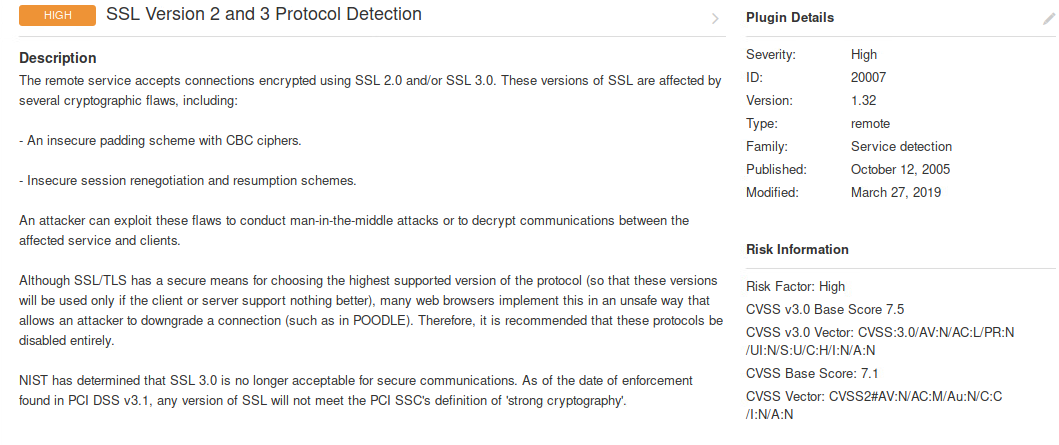
Nmap scan to see which IP is saturna. Result is 172.16.0.13zenmap topology of SaturnaN(172.16.0.13) and SaturnaR(172.16.0.14)open ports of SaturnaNopen ports for SaturnaRSaturnaN information SaturnaR info

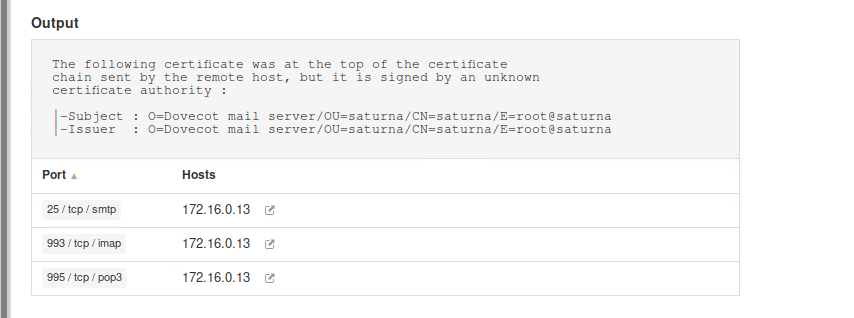
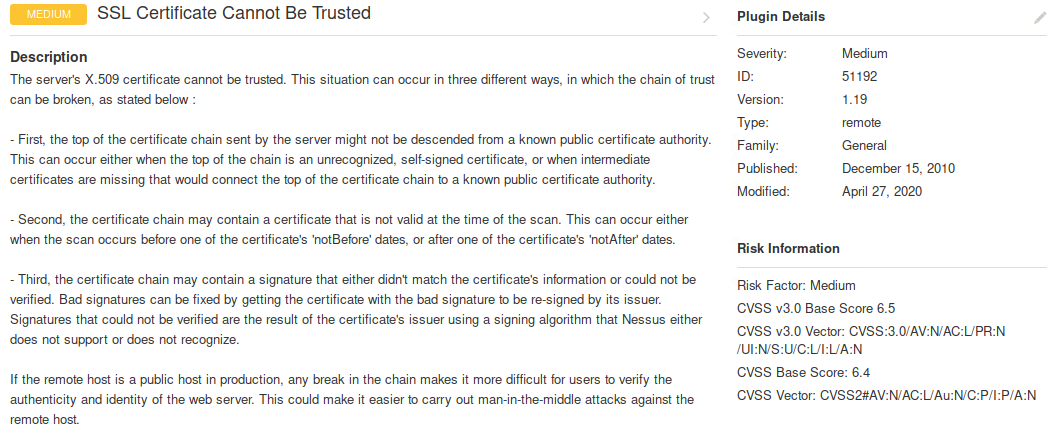
SaturnaN vulnerabilities as shown on Nessus



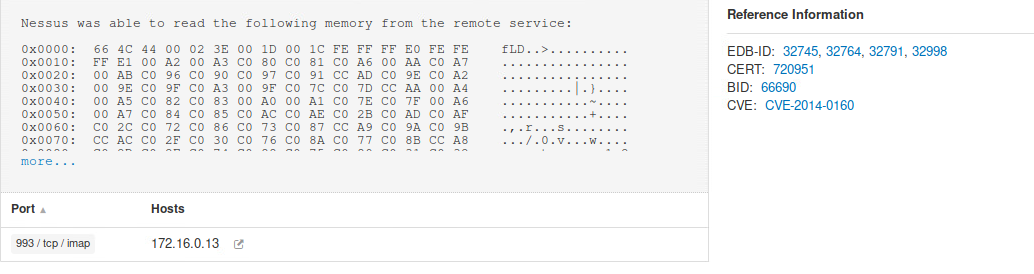
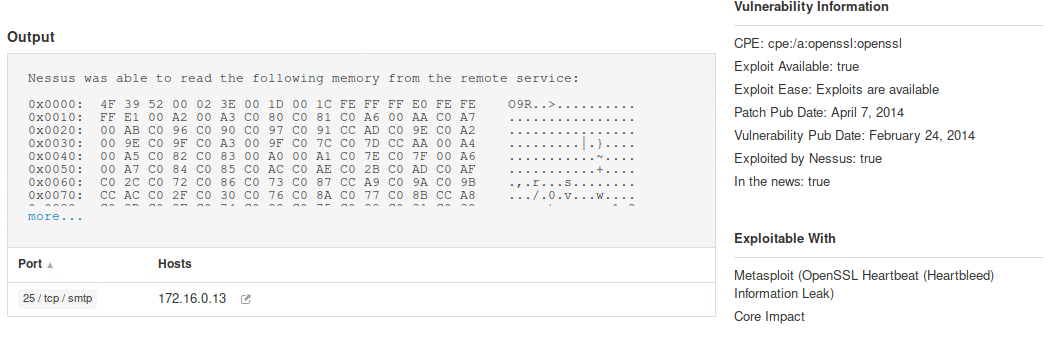
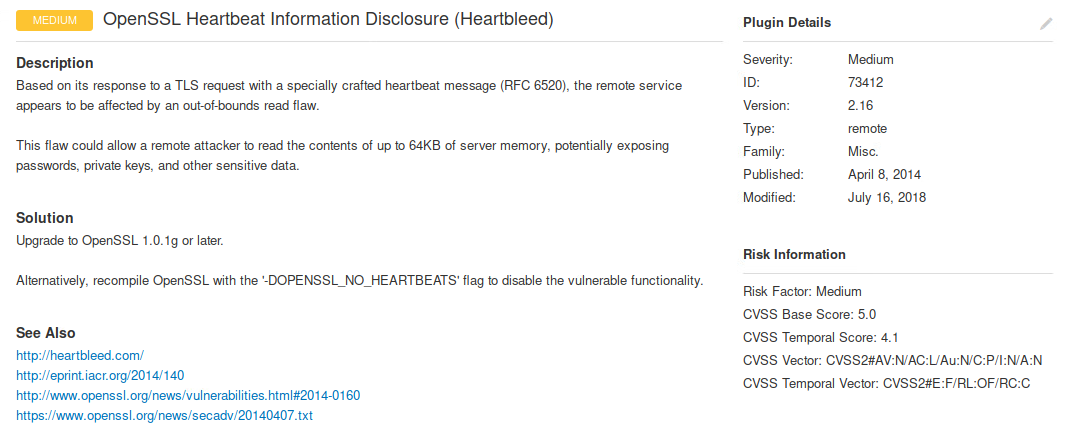


Example 1:The operating system is unsupported and could have holes in its security because the holes that were discovered during and after its active period are accessible through programs like metasploit and can be used to attack.

Example 2:This version of SSL is considered unreliable because it provides unreliable session renegotiation and could lead to man in the middle attacks and attackers could decrypt the communication between the users.

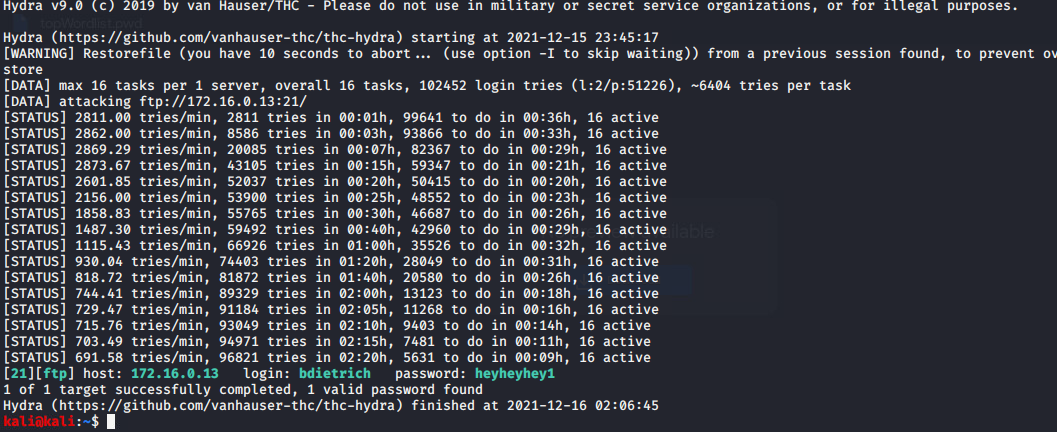
Example 3:

Without a recognizable or trustable certificate, it is hard to identify and trust the server that you are connecting to and can lead to man in the middle attacks against your remote host.

Example 4:

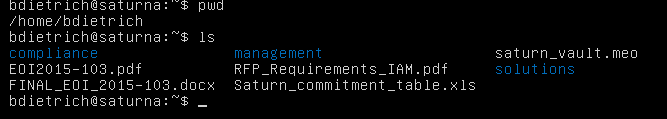
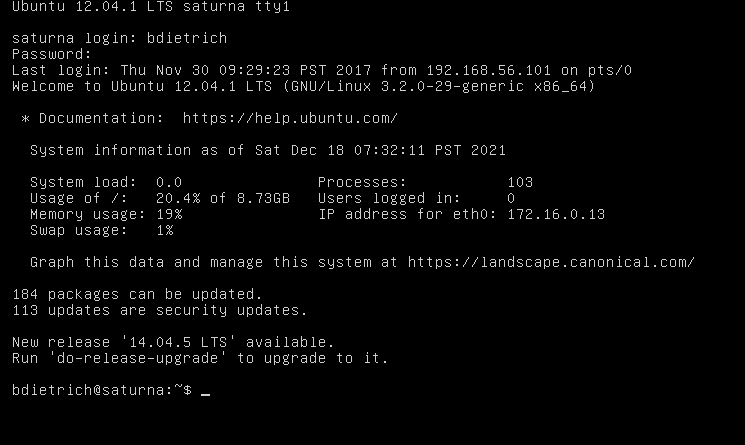
This vulnerability can allow attackers to read small blocks of information that can range from something useless as a time-stamp to very important information such as keys or passwords.

Password cracking through the use of hydra



Password result is heyheyhey1

SaturnaN login

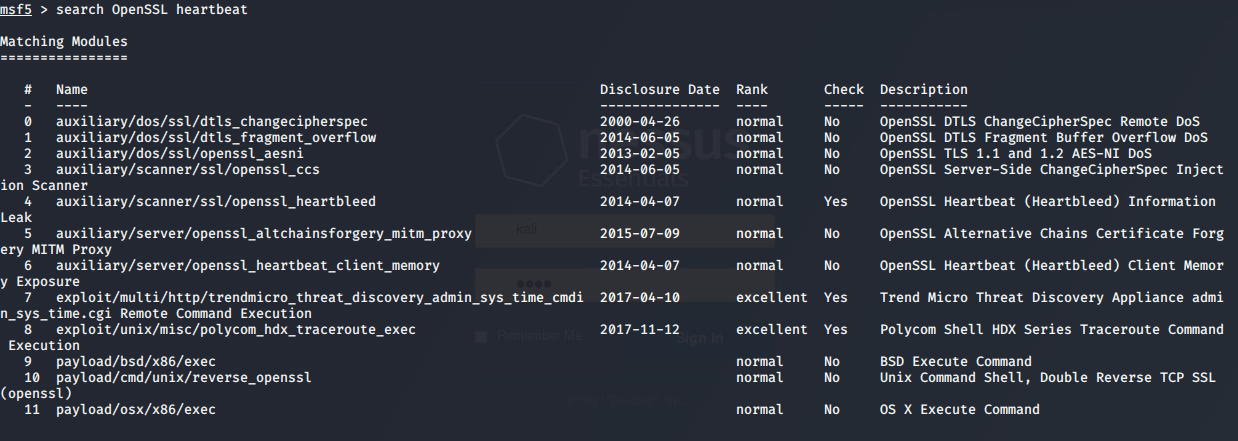


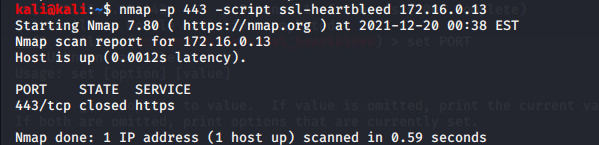
Part 2:  
1.

The heartbleed bug is a result of an error in the OpenSSL code which is a popular code library for implementing HTTPS encryptions in things such as websites and e-mail servers and many other things. Due to a missing bounds check in the source code, this bug allows attackers to recover large amounts of code by repeating the action of sending code to the server. The attacker can only grab up to 64kb of information but that is still enough to be able to grab information of things ranging from time-stamps to key and passwords.

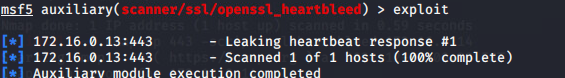
The bug comes from the TLS heartbleed extension where it is missing a bounds check in the request. An attacker can receive the information by specially crafting a TLS heartbleed request. The request contains a type, payload length, payload and padding. The bug comes from it never checking the payload length to the request packet so the attacker can craft the TLS heartbleeds payload length and receive information from the client or server.





Nessus states that the exploit is available but nmap states that port 443 is closed 

In which case I can not use the exploit provided on metasploit to use information gained from heart bleed



Some snort rules I can add without too much testing being able to be done as I am running out of time are:

Alert tcp any any -> any any (msg:”OpenSSL Heartbleed”; flow:established; reference:cve,2014-0160; sid1234566;)

Tcp is the proto because heartbleed goes through the https port which is 443 and so we can change the rule to

Alert tcp any any -> any 443( msg:”OpenSSL Heartbleed”; flow:established; threshold:type limit, track by\_src, count 1, seconds 600; reference:cve,2014-0160; sid1234566;)

Established check to see if the connection is established. Reference is used to reference the cve code of heart bleed.

We can also specify $EXTERNAL\_NET and $HOME\_NET making the rule

Alert tcp $EXTERNAL\_NET any -> $HOME\_NET 443 (msg:”OpenSSL Heartbleed”; flow:established; threshold:type limit, track by\_src, count 1, seconds 600; reference:cve,2014-0160; sid1234566;)

The count allows for one connection and will notify if it goes over 10 minutes.

IPTABLE rule would be

Iptables -A INPUT -p tcp --dport 443 -j DROP

This will stop all input from 443 but we do not want this so it would be

Some other ways to improve the fire wall would be to look through the alerts by snort and drop any IP addresses that are shown to use the exploit

For the safety of the system, it is best that the system is updated to the newest option as that will resolve many of the security flaws in the system