**Vulnerability scanning**

1. **Vulnerability in the Linux VM:**

- Vulnerability type MEDIUM

- Vulnerable Cipher Suites are being used for HTTPS. Services like TSLv1.0, TSLv1.1, TSLv1.2 are accepting vulnerable ciphers that can be broken.

- The cipher suite TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA is being used by the aforementioned services. This suite uses the 64-bit block cipher Triple-DES, which is vulnerable to the SWEET32 attack commonly known as the Birthday attack.

- The short block size (64-bits) makes the block cipher vulnerable to the Birthday attacks. The attacker may send large amounts of dummy data and get blocks of cipher text that match the user/customer. It is possible because the 64-bit blocks used by ‘Triple-DES’ generate a lot of packets. This increases the probability of an encrypted packet of the user and that of the attacker matching.

- These attacks can be mitigated by changing the configuration of these SSL/TSL services so that they do not accept the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite. Or we could limit the length of the TLS session using a 64-bit cipher.

- We could also disable the use of cipher suites using Triple-DES.

**Vulnerability in the Windows VM:**

- Vulnerability type MEDIUM

- Distributed Computing Environment/ Remote Procedure Calls or MSRPC services running on the host can be **enumerated** by connecting on **port 135** and doing the appropriate queries.

- Enumeration in information security is the process of extracting the user names, machine names, network resources and other services from a system. All the gathered information is used to identify vulnerabilities or weak points in the system.

- An attacker can use this fact to gain more knowledge about the host.

- We can mitigate this by filtering the incoming traffic to the ports which are running the DCE/RPC or MSRPC services. And by closing any unnecessary service that can be enumerated.

- Or we could use TCP Wrappers. These give the network administrator the flexibility to permit or deny access to the services based on IP address or domain name.

1. **Vulnerabilities on 10.0.0.113 (knoxville.nslab):**

- Vulnerability type HIGH

- The host is missing a **critical security update** according to the Microsoft Bulletin (MS09-001). The issue is due to the way that the Server Message Block (SMB) Protocol handles specially crafted SMB packets.

- Successful exploitation of this vulnerability would allow **remote code execution** on the server. Any unauthenticated adversary to cause a denial of service by sending a specially crafted network message to the system running the server service. Most attempts to exploit this vulnerability would lead to a denial of service but the attacker could achieve remote code execution, which in turn will lead to the attacker taking complete control of the system.

- In order to patch this vulnerability, we could simply install the software updates. We could do this by running the Windows Update and update the listed hotfixes.

**Vulnerabilities on 10.0.0.124 (chicago.nslab):**

- Vulnerability type HIGH

- The “Debian/GNU Linux” Operating System on the host has reached the end of its life and should not be used anymore. End of Life date: 29-02-2016.

The expired OS will no longer receive any security updates. Unfixed vulnerabilities may be used by an adversary to compromise the system.

- This vulnerability can be fixed by updating the Operating System to the latest version of the chosen “Debian/GNU Linux” Operating System. The new OS will receive all the new security updates, which will have patched various vulnerabilities in the system.

1. The efficiency of vulnerability scanners depends on the following factors:
2. Frequency and method for plugin updates-

Usually a vulnerability scanner cannot identify a vulnerability if its corresponding plugin is not available. For instance, if we do not update our feed of the Network Vulnerability Tests then OpenVas will not be able to find some vulnerabilities. Simply because it never tested for them. As a result, faster the vendor can update and add new plug-ins, more capable the scanner will be of spotting new flaws. If a scanner has the option for automatically updating and installing the new plug-ins, then it has more chances of spotting new vulnerabilities.

1. Quantity versus quality of the vulnerabilities detected-

The accuracy with which the high risk vulnerabilities are detected is more important than the number of vulnerabilities checked, because the same vulnerability may be recorded multiple times.

**Vulnerabilities fixed:**

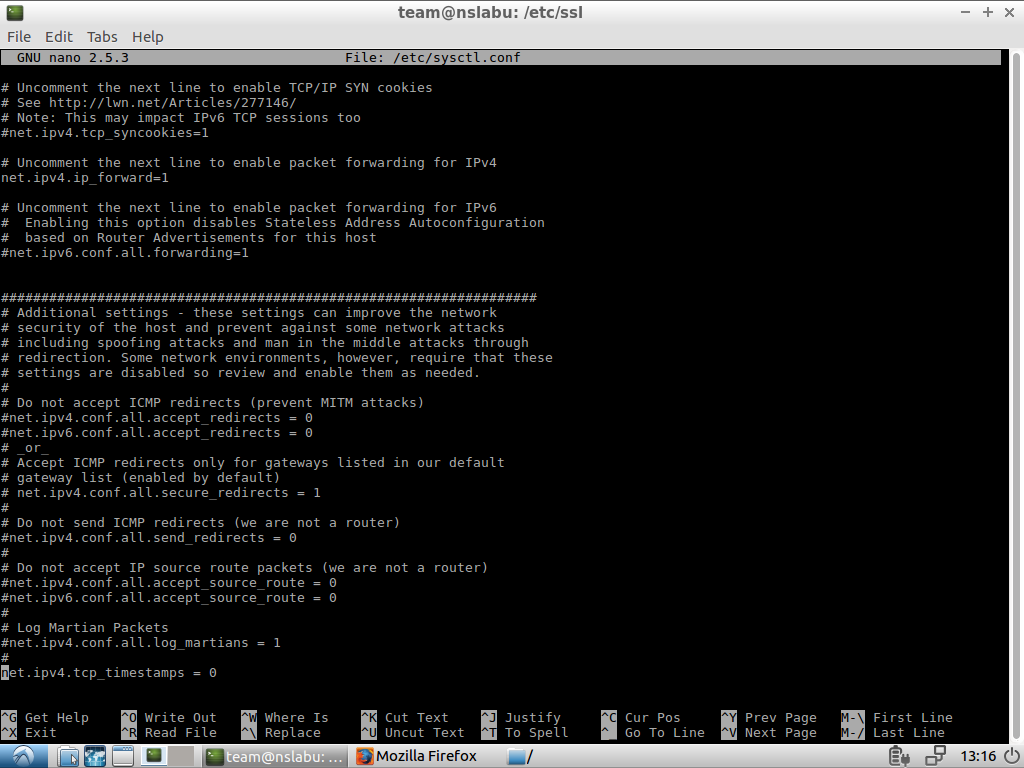
In Linux VM:

1> The host implements TCP timestamps, hence allowing the adversary to compute the uptime.

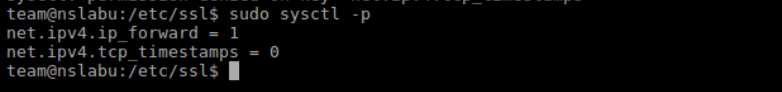
- Vulnerability type LOW

- An adversary can use this exploit to get information about how much time the host was running/ active.

-We disabled the TCP timestamp on the Linux machine by adding the line ‘net.ipv4.tcp\_timestamps = 0’ to the /etc/sysctl.conf



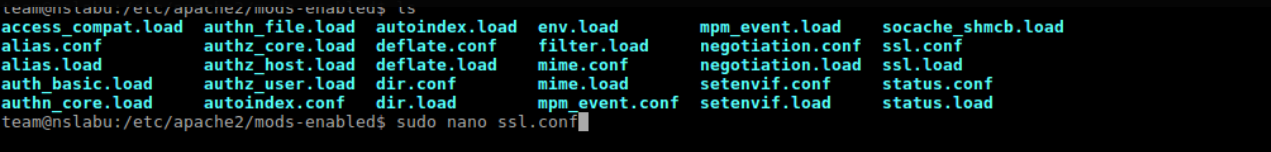
-Then we run the sysctl -p command to apply the settings at runtime.

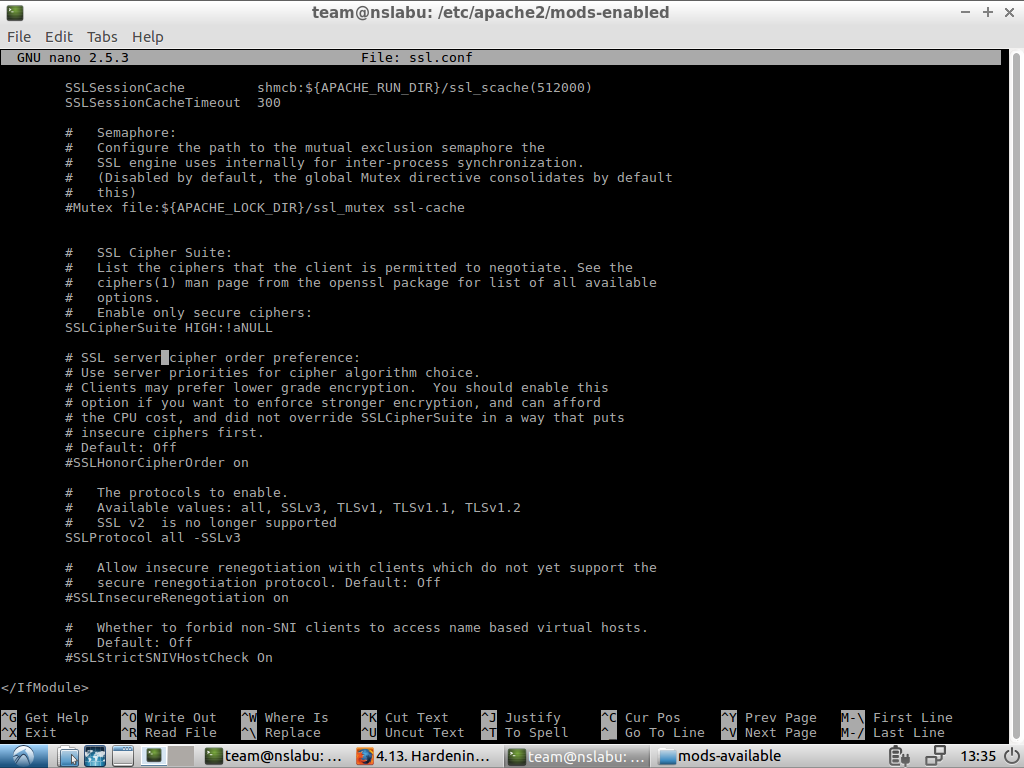


2> Apache HTTP server using vulnerable cipher suite and old versions of SSL.

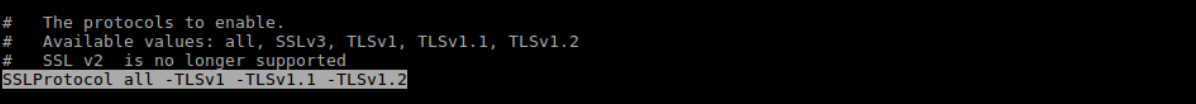
- Vulnerability type MEDIUM

- The apache HTTP server was using SSLv3 and the cipher suite TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA , which is known to be vulnerable to the SWEET32 attack also known as the birthday attack. This is because they use ‘Triple-DES’ which is a block cipher and uses blocks of size of 64-bits.

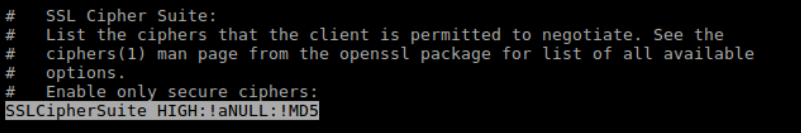




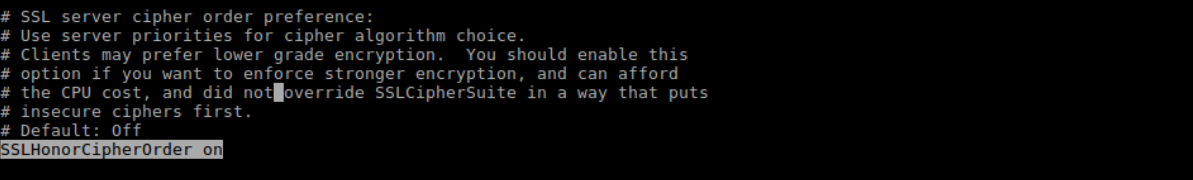
- We mitigated this vulnerability by disabling support for SSLv3 and changing it to TLSv1, TLSv1.1 or TLSv1.2.



- We make sure that we are using cipher suites that are defined as belonging to the HIGH group. This group discards all the cipher suites that are known to be broken or weak.



- Finally, we make sure that the Cipher order is honoured by the client, so that the client will use server priorities for cipher algorithm choices. This will enforce stronger encryption.



In Windows VM:

The host implements TCP timestamps, hence allowing the adversary to compute the uptime.

- Vulnerability type LOW

- An adversary can use this exploit to get information about how much time the host was running/ active.

-We disabled the TCP timestamp on the Windows VM by running the command

‘netsh int tcp set global timestamps = disabled’ as administrator.

